Lithuanian National Risk Assessment of Money Laundering and Terrorist Financing

2015, Vilnius

Table of contents

Abbreviation	Name & Detail
AML/CTF	Anti-Money Laundering / Counter Terrorism Financing
ML/TF	Money Laundering / Terrorism Financing
NRA	National Risk Assessment
RBA	Risk-Based Approach
ML	Money Laundering
TF	Terrorism Financing
FATF	Financial Action Task Force
EU	European Union
UN	United Nations
OFAC	Office of Foreign Assets Control
PEP	Politically Exposed Persons
STR	Suspicious Transaction Report
DNFBP	Designated Non-Financial Businesses and Professions

1. Introduction

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Illegal arms sales, smuggling, and the activities of organised crime, including for example drug trafficking, can generate huge amounts of proceeds.

Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

The United Nations Office on Drugs and Crime (UNODC) conducted a study to determine the magnitude of illicit funds generated by drug trafficking and organised crimes and to investigate to what extent these funds are laundered. The report estimates that in 2009, criminal proceeds amounted to 3.6% of global GDP, with 2.7% (or USD 1.6 trillion) being laundered. This falls within the widely quoted estimate by the International Monetary Fund, who stated in 1998 that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world's gross domestic product. Using 1998 statistics, these percentages would indicate that money laundering ranged between USD 590 billion and USD 1.5 trillion. At the time, the lower figure was roughly equivalent to the value of the total output of an economy the size of Spain.

However, the above estimates should be treated with caution. They are intended to give an estimate of the magnitude of money laundering. Due to the illegal nature of the transactions, precise statistics are not available and it is therefore impossible to produce a definitive estimate of the amount of money that is globally laundered every year.

As money laundering is a consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launderers tend to seek out countries or sectors in which there is a low risk of detection due to weak or ineffective anti-money laundering programmes. Because the objective of money laundering is to get the illegal funds back to the individual who generated them, launderers usually prefer to move funds through stable financial systems. Economies with growing or developing financial centres, but inadequate controls are particularly vulnerable as established financial centre countries implement comprehensive anti-money laundering regimes. Differences between national anti-money laundering systems will be exploited by launderers, who tend to move their networks to countries and financial systems with weak or ineffective countermeasures.

The possible social and political costs of money laundering, if left unchecked or dealt with ineffectively, are serious. Organised crime can infiltrate financial institutions, acquire control of large sectors of the economy through investment, or offer bribes to public officials and indeed governments.[1]

Because of those threats, countries put in place measures seeking to take illegal proceeds from criminals, disclose predicate crimes, implement money laundering prevention measures, access and evaluate money laundering risks in national context.

In response to mounting concern over money laundering, the Financial Action Task Force on money laundering (FATF) was established by the G-7 Summit in Paris in 1989 to develop a co-ordinated international response. One of the first tasks of the FATF was to develop Recommendations, 40 in all, which set out the measures national governments should take to implement effective anti-money

[1] Text above is taken from official FATF website http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223

laundering programmes. After the 9/11 events on 2001 FATF develops recommendations in the sphere of prevention of terrorist financing as well.

Lithuania is a member of MONEYVAL. The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards - FATF recommendations.

One of the most fundamental FATF standards is a requirement for countries to identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively.

Identifying, assessing, and understanding ML/TF risks is an essential part of the implementation and development of a national anti-money laundering / countering the financing of terrorism (AML/CFT) regime, which includes laws, regulations, enforcement and other measures to mitigate ML/TF risks. It assists in the prioritisation and efficient allocation of resources by authorities.

This is the Lithuania‘s first money laundering and terrorist financing national risk assessment (NRA). NRA was conducted together with a private partner “Deloitte Lietuva” in period of year 2014 to 2015.

All NRA process was controlled by high level AML\CFT Coordination Group was created by the order of Prime Minister No 42 of March 2 of 2015 consisting of high rank officers from all involved institutions:
Government of the Republic of Lithuania;
Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania (FIU);
Ministry of Justice;
Ministry of Finance;
Ministry of Interior;
State Security Department of the Republic of Lithuania;
Bank of Lithuania;
Customs Criminal Service under the Ministry of Finance;
Department of Cultural Heritage Protection under the Ministry of Culture;
State Gaming Control Service under the Ministry of Finance;
Chamber of Notaries;
Chamber of Auditors;
Lithuanian Chamber of Bailiffs;
Lithuanian Assay Office;
State Tax Inspectorate under the Ministry of Finance;
Lithuanian Criminal Police Bureau;
Special Investigation Service;
General Prosecutor Service;
Lithuania Bar Association.

On October 28th of 2015 the Working Group approved Lithuania‘s NRA report, conducted by „Deloitte Lietuva“ and Lithuania state institutions.

2. Methodology

The National Risk Assessment is the important step to take in order to enhance the AML/CTF national system.

The NRA addresses all stakeholders with responsibilities in applying the AML/CTF national and international legal framework. The national public and private institutions must co-ordinate their actions in order to establish an effective AML/CTF system.

The assessment is performed in accordance with the current context and conditions. Even if the assessment may follow a certain pattern, the identified risks will reveal the present situation; therefore the goals and objectives of the risk assessment must be defined taking into consideration the current uncertainties, vulnerabilities and exposures, in order to determine an action plan for combating the threats and improving the weaknesses of the AML/CTF system.

The national risk assessment follows its objectives and goals and provides a basis for decision-making, the grounds on which the stakeholders can build strategies for enhancing the internal processes.

In performing the risk assessment, there are 5 stages in managing the national AML/CTF risks:

- Data collection;
- Risk identification;
- Risk assessment;
- Risk response measures;
- Risk management plan.

The project begins with complex processes that concern collecting data and information that will help on identifying the risks that may affect the AML/CTF system and then, determine their characteristics and their nature.

Identification of possible risks is an activity that is performed not only in the beginning of the assessment, but also following the next stages, as the process is a dynamic one as risks may arise and entail others while analyzing the available data. The risks that have been revealed are analyzed in order to establish their characteristics and categorize them in order to establish their nature. In this phase, assessor identifies inherent risks, which are related to the assessment's objective and occur without the interference of mitigation measures or controls.

Assessors create Risk Registers in order to keep track of the data and records regarding the identified risks, containing all information and data gathered while performing the NRA. The risks are assigned to stakeholders as risk owners, based on their attributions and responsibilities in order to be properly managed.

Using checklists is a technique that can recognize risks for which an assessor may already have a response. If there is the case, eventual responses must be written down in order to use them as a start point in following processes.

The assessment continues with the analysis of the risks in order to establish their relevance, their priority and the stakeholder's attitude towards them. In this respect, the assessor must establish risk's likelihood of occurrence, its impact it may have when it will occur and vulnerability caused by the risk.

Based on the analysis of those three elements, the assessor can approach the risks by their priority, in accordance with the stakeholder's risk attitude. The assessor, together with the stakeholders, use a risk matrix tool for understanding the size of the consequence and its likelihood of occurrence and caused vulnerability of the AML/CTF system.

The risk attitude implies setting out the tolerance level, developed by interviewing the stakeholders. Based on the analysis performed using the risk matrix, the risks that have minor impact and probability and for which no further actions should be taken, are included in a Low Risk Watch List, which is further monitored by the stakeholders. If the monitoring process reveals that these risks' priority has risen, they are removed from this list and follow all the risk assessment's phases and steps.

After finalizing the risk analysis, the assessor must establish the risk response plan. In this respect, the analysis results help on choosing the most appropriate strategy to respond to risks, hence choosing to avoid, share, mitigate or accept the risks.

2.1. STAGE 1 – Data collection

In order to identify the country ML/TF risks it is necessary to collect data from all relevant stakeholders through surveys, direct interviews based on prior developed questionnaires, gathering statistical data on the threats and vulnerabilities regarding political, economic, financial, legal and law enforcement factors.

The information collected is not always relevant to the assessment. Therefore, it needs to be analyzed and processed in order to establish which data contains facts and circumstances that can represent a threat or vulnerability for the AML/CTF system. The objective of this process is to capture an accurate view of the setting in which the AML/CTF risks arise. The targeted areas are various, as well as the methods with which the gathering process may proceed.

In order to achieve the assessment's goals and objectives, it is mandatory to understand the national context from the economic, political, social, legal, environmental and technological points of view. Money launderers and terrorists may take advantage of any loophole of the systems and this obliges authorities to take preventive measures in all sectors.

Risk identification is a dynamic, ongoing process, which must not be limited only to the first assessing phases. New risks may arise while analyzing ones firstly identified, therefore an assessor should consider all information, data or hypotheses while performing the assessment. Moreover, assessors should consider focusing on finding the risk's causal factors, which will help on identifying the proper strategies and actions that are to be taken in order to ensure that the objectives of the assessment is realized. This will also help on categorizing the risks that have the same causal factors in order to apply a similar risk management plan.

In pursuing this stage of the risk assessment, the assessors must get through documentation reviews, relevant to the assessment. The materials can be found on publicly available sources or can be requested to the authorities to which the assessment is destined. The reason why this method helps identifying risks is that each document is reviewed for completeness and consistency, in accordance with standards and legal provisions. It also helps on understanding the processes and procedures inside the system and the circumstances in which risks may arise.

The main sources of information include:

1. AML/CFT Legislation of Lithuania;
2. International Conventions, recommendations or guidelines (for example, UN Conventions, EU legislation, FATF Recommendations, guidelines issued by the Basel Committee on Banking Supervision, etc.);

3. Moneyval reports and recommendations;
4. Reports of Lithuanian FIU, regulatory and supervisory bodies, professional associations responsible for the implementation of AML/CFT legislation;
5. Responses to questionnaires/surveys;
6. Information received during interviews with stakeholders;
7. Statistics on the number of STRs, sanctions, ML/TF investigations, convictions, confiscations, etc.
8. National and international mass media (it is recommended to take the media reports only as hints and indications – for further research), etc.

In performing the risk assessment, the stakeholders should use and verify all the available data and financial information.

2.2. STAGE 2 – Risk identification

The AML/CTF system must ensure that the risks of committing money laundering and terrorist financing are kept under control by applying preventive measures and following actions plans.

In this respect, assessors must analyze and collect information in order to identify the events and circumstances that might represent a risk to the AML/CTF system, using, if applicable, one or more of the following methods and techniques:

- Brainstorming. This is a straightforward identification technique that uses experts for the purpose of gathering and listing as many ideas as possible. It is a very efficient method because experts use each other's line of thought to lead them in identifying new risks. In a brainstorming session, no matter how insignificant or irrelevant the idea is, it will be listed in order to create hypotheses that may help in revealing precise risks. The only condition is that the experts who participate should go through documentation reviews prior to the brainstorming session, in order to obtain maximized results.
- Delphi technique. This method is performed using interactive forecasting actions carried out by a group of experts using questionnaires. The experts answer the questions giving justifications to their opinions in several rounds, having the opportunity to revise or change their answers, until everyone reaches a general agreement on the subject. Once again, the experts must prior go through documentation review in order to give pertinent answers to the questionnaires.
- Surveys, questionnaires and interviews. These tools are very useful for gathering information directly from the individuals or entities with key positions inside the AML/CTF system.
- Assumption techniques. This method implies testing the accuracy, instability or inconsistency of assumptions, hypotheses and what-if scenarios which will help the assessor identifying risks. If the assumptions do not match the given data and facts, then it will be easy to identify which are the sectors that may be endangered by threats.
- Checklist analysis. This method uses structures and records from previous projects that help identifying most of the significant risks. It can be used after the relevant data and information are gathered, as a basis on which the analysis can be performed. The checklist technique is not sufficient, although, as it does not cover all the current risks and does not provide an updated outlook of the national context.

2.3. STAGE 3 – Risk assessment

In this stage, the assessor must analyze the identified risks in order to determine what actions are to be taken for managing the threats and vulnerabilities of the system.

It is also important to consider the fact that, from analyzing the available data, other risks may arise during the process of the risk assessment. Therefore, the stages may not be entailed from the first one to the last one, assessors might come back to first stage and go through all phases once again in order to come to maximized results. Hence, the process should be a flexible one, taking into consideration all uncertainties that may occur while performing the NRA.

The first step in analyzing risks is to establish the precision of the used data and information. The identified risks should have a clear and sustainable basis on which the assessment should be built on. Hence, in establishing data precision, an assessor must take into consideration the fact that the understanding of the risks and their context must be at a high level, in order to make an accurate analysis and to apply the most appropriate risk response measures. Thus, there should be enough data and information on the risk and the contextual setting in which it has been identified, ensuring that the sources from which the information has been extracted are reliable and of a high quality. As an example, a threat which has been identified from a national report issued by the National Bank will have more credits than the one that has arisen from a media report. However, the analysis will concern all identified risks that an assessor identifies.

Risk Priority is set by determining the risk's likelihood of occurrence, its impact and the vulnerability of the system. The analysis implies combining those three aspects and determine which risks should be further monitored and which risks should go directly into the risk response stage. It is recommended to build a matrix in which risks are rated from these three points of view.

Risks that have been low rated are included in the Low Risk Watch List and are not further assessed, but they are further monitored.

After assessing the vulnerability and their probability and impact, an assessor should prioritize the risks. This prioritization will be the basis of the risk response process.

Assessors must clearly understand the country risk tolerance in order to succeed in giving the most appropriate risk responses and understand the amount or level of risk the stakeholders can withstand.

Risk tolerance is established using interviews, questionnaires. Also, previous experience in risk management might help the assessor and the stakeholders, to establish the risk threshold.

The identified risks which are positioned above the threshold line must be responded or take caution in managing them. For the national AML/CTF risk assessment, stakeholders must not have a high tolerance in taking risks, as their impact might take effect in the political, economic or legal systems. However, stakeholders should not consider a low tolerance either, as it may cause negative effects on the political, economic and legal development.

After this step, the assessor proceeds on updating the Risk Registers with the information arisen so far from the risk assessment. The added information will concern the contextual setting in which the risks have been identified, the causal factors, the vulnerability, the probability, the impact, the priority rank.

2.4. STAGE 4 – Risk response measures

The assessor needs to visualize the issues found before proceeding on a response plan. He must assign the identified risks to the stakeholders, based on their attributions and responsibilities and establish the

risk owner. The stakeholders then assign a person that is responsible in managing that risk, by applying the risk response measures, monitoring and control.

Planning risk responses implies an analysis of the impact of the risk in comparison with the cost that the response may concern.

For diminishing the risk exposure, the assessor may choose the following actions: avoidance, sharing, mitigation and acceptance.

Avoiding the risk. This strategy applies when the consequences of simply removing the risk would be minor. For example, financial institutions may consider not initiating business relationships in countries that are not considered cooperative from the AML/CTF point of view or for which international sanctions have been established.

Sharing the risk. This is a strategy for transferring/sharing a portion of the risk with third parties that would accept this option. However, this action does not eliminate the risk and only shifts the responsibility to another subject.

Mitigating the risk. This strategy concerns diminishing the risk's consequence by mitigating the risk's probability, impact or both. Stakeholders should be aware of the fact that preventing a risk before it occurs is more effective than restoring. This implies building an elaborate action plan that will consider reducing the risk not only on short term, but mitigate the risk's impact and probability so that its consequences would be at an acceptable level. For example, if a financial institution opens a branch in an AML/CTF non-compliant country, that branch might suffer serious operational and reputational risks. In this respect, it may enhance its prudential policies and adopt more restrictive procedures and processes in order to ensure a safe environment.

Accepting the risk. For those risks that do not cause significant consequences and are ranked below the risk threshold, stakeholders may decide on accepting them. Those risks are low in probability and impact. The acceptance strategy may have an active or a passive approach. Passive acceptance implies taking no action and simply bearing the risk's impact. Active acceptance concerns developing a contingency plan for when the risk will occur. This means establishing an action plan, which can be pursuit in case of occurrence. For example, an institution is aware of the risk for a client to have a false identity, even if it has implemented customer due diligence procedures and processes in the internal policies. Still, the bank opens accounts. This is an accepted risk. However, the Financial Institutions internally regulates what steps are to be taken if the customer proves to have a false identity. This is an active risk acceptance.

In this stage, options are analyzed in order to ensure that the damage caused by a risk can be acceptable for the AML/CTF system. Highly restrictive response measures may inflict other risks or consequences from other points of view. For example, if the National Bank issues strict and non-flexible regulations and dispositions for the commercial banks, then the risk of economical and investment blockage may arise. In this respect, the assessor must have an appropriate level of AML/CTF expertise and a wide perspective on the national system in order to take the right decisions in responding to risks.

The outcome of this stage will be the risk response plan, which will help the stakeholder understand how to manage the risk it owns. After establishing an action for managing the identified risks, the next step is to monitor the risk management in order to pursuit the assessment's goals and objectives.

2.5. STAGE 5 – Risk management plan

The last stage of the risk assessment implies developing a plan for supervising the implementation of the risk responses and the execution of the risk management plan. This is an ongoing process until the next risk assessment.

As stated before, risk management is about taking the best decision for complying with the legal requirements and not affecting the political or economic areas. All the participants in the AML/CTF risk assessment must understand that AML/CTF risks are not about gains and losses, but about compliance or not with the international standards. The consequences may be economical, political, legal, and all at a national level. That is why it is so important to achieve the assessment goals and objectives and establish a risk control and monitoring plan in order to ensure that the threats and vulnerabilities that might represent a danger to the system are suppressed.

The identified risks must be kept under observation, even the ones that have been introduced in the Low Risk Watch List. Not only must the risks be monitored, but also their causal factors, in order to establish if there is any chance for other risks to arise.

Furthermore, implementing proper monitoring measures will help the assessor and the stakeholder on determining if risk response measures are effective and if they reduce the extent of the risk to the level of tolerance.

In this respect, stakeholders must ensure internal and external audits and controls to examine the execution of the processes and the risk response performance. As a result, risk management can be evaluated and enhanced by using internal controls, tests on the system, checklists and other tools and techniques. Supervision authorities have also an important role in the evaluation of the system.

Stakeholders must periodically reassess the initial identified risks and the ones that have arisen while pursuing the risk management plan.

Stakeholders must also perform periodical AML/CTF risk assessments in order to confirm whether current risk assessment results should remain the same.

Assessors and stakeholders must always update the Risk Registers with all the changes and new information that resulted from performance of risk response measures, etc.

2.6. NRA Process

Deloitte together with the FIU and the stakeholders performed the NRA following the Methodology described in this Chapter.

In this respect, for understanding the context and circumstances in which ML/TF risks may arise and affect Lithuania, Deloitte team developed the questionnaires with the purpose of gathering enough information not only on experts' opinion, but also on statistics, in order to create a historical data portfolio to start with the NRA.

Based on the stakeholders' responses to our AML/CTF questionnaires and on the Moneyval reports, statistics were gathered, which helped to identify the vulnerabilities and the inconsistencies of the Lithuanian AML/CTF System.

In addition, Deloitte team has reviewed the publicly available documentation on Lithuania, as described in *Appendix 1 – "Credible Sources"*, for obtaining an understanding on all the circumstances and contexts that may serve as a causal factor for ML/TF risks.

The responses to questionnaires and the documentation review offered a basis on which the interview plans were created. The Deloitte team has scheduled interviews with all relevant stakeholders, for clarifying any uncertainties arisen from the questionnaires and for identifying new inherent risks. The interviews were scheduled as presented in *Appendix 2 – "Interviews with the stakeholders"*.

Deloitte experts further performed a Brainstorming session, in order to understand and analyze the gathered information and to develop a *Risk Register*. The risks were classified by their causal factors.

Having the risks categorized, Deloitte experts assigned them to a Risk Owner, in accordance with all the stakeholders' attributions and responsibilities in matter of AML/CTF.

Deloitte ended the identification process, together with the FIU and the stakeholders, by creating a final version of the list of identified risks, as presented in the *Appendix No. 4 – "List of Lithuanian ML/TF risks"*.

2.7. Risk scoring matrix

The risk scoring matrix was developed as described, which prioritized the identified risks by calculating impact, probability and vulnerability, taking into consideration the following:

- The impact represents the cost/damage if the risk occurs;
- The probability represent the chance of the risk to occur;
- The vulnerability represents the efficiency and effectiveness of current controls used for mitigation of risk impact and/or likelihood.

The following areas of impact caused by AML/CTF risks were determined:

1. National Security;
2. Economic and social situation;
3. Country reputation;
4. Criminological situation.

Deloitte together with the FIU and the stakeholders ranked the risks in accordance with the risk scoring matrix. Risks scores have been determined as follows:

- The probability, impact and vulnerability were ranked by scoring each of them with values from 1 to 5;
- The risk ranking was calculated by adding the probability, impact and vulnerability scores to a total score;
- The risk priority was established in accordance with the total score of the risks: *High priority* (scores from 10 to 15), *Medium priority* (scores from 5 to 9) and *Low priority* (scores of 3 and 4).

Therefore, the risks can receive a minimum total score of 3 and a maximum total score of 15.

Measure	Rating scale	1	2	3	4	5
		Very low	Low	Medium	High	Very high
Impact	National security	Insignificant impact to national security	Petty corruption in public sector	Corrupted environment at the national institutions and authorities level	- Damage on the computer systems and databases - Loss or disclosure of classified information	- Intensive cross-border passing by people associated to terrorism groups - Damage on communication systems - Damage on infrastructure systems - Damage on ethic and cultural property
	Economic and social situation	Insignificant economical impact	- Foreign investment minor affected. Small decrease, up to 5% - Liquidity problems due to withdrawal of funds - Decline of the stock value of financial institutions	- Foreign investment decreased (up to 30%) - Impact to country economic growth which is slower in comparison with the rest of EU countries by 10% - Transformation of productive enterprises into sterile investments (by operating them for laundering illicit proceeds) - Corrupted environment at the financial sector level - Loss of profitable business - Uneven social and economical development - Increase rate of shadow economy	- Foreign investment significantly decreased (up to 80%) - Major impact to country economic growth which is slowed down significantly in comparison with the rest of EU countries - No trust of country's banking system (customer mistrust in the financial sector) - Sharp surge in financial sector, followed by sharp decline, resulting in macroeconomic instability - Significant drop in asset prices - National loan losses	- No foreign investment - Country fiscal policy is significantly impacted with weak collection of the budget - Exclusion from access to the major financial institutions and markets - Country economic growth is stopped - Misleading country macro and micro statistical data - Closure/crash of financial markets
	Country reputation	Insignificant impact to country reputation	Disputes, proceedings with regulators with no public media occurrence	- Isolated instances of sanctions by regulators with local public media occurrence - Closure of business relationships - High rate of emigration	- Occurrences of criticism in international media - Sanctions by regulators	- Recurring sanctions and other limits to the country imposed by regulators that affect country's functioning significantly and bear very high cost to assure compliance - Counter-measures imposed by FATF against Lithuania - Permanent criticism in international media - Being placed in the "non-cooperating countries and territories" by ICRG
	Criminological situation	Insignificant to criminological situation.	- Fraudulent activities undertaken by employees - Increase rate of 5% on predicate crimes (such as: illegal arms sales, smuggling, drug trafficking, prostitution)	- Increase rate of 15% on predicate crimes (such as: illegal arms sales, smuggling, drug trafficking, prostitution)	- Increase rate of 25% on predicate crimes (such as: illegal arms sales, smuggling, drug trafficking, prostitution) - Cross-border contamination of	- Increase rate over 30% on predicate crimes (such as: illegal arms sales, smuggling, drug trafficking, prostitution) - Destruction of life and property
Likelihood		Event occurring less frequently than once a year	Event occurring less frequently than once in six months	Event occurring less frequently than once in a quarter	Event occurring at least once a month	Event occurring daily
Vulnerability		Actions that are being undertaken practically fully eliminate impact and/or likelihood (if possible to estimate, efficiency over 90%)	Actions that are being undertaken mostly mitigate risk impact and/or likelihood (if it is possible to estimate, effectiveness in range 80%-89%)	Actions that are being undertaken partly mitigate risk impact and/or likelihood (if it is possible to estimate, effectiveness in range 70%-79%)	Actions that are being undertaken not fully mitigate risk impact and/or likelihood (if it is possible to estimate, effectiveness in range 50%-69%)	Actions that are being undertaken are ineffective or it is not possible to mitigate risk impact and/or likelihood (if it is possible to estimate, effectiveness not higher than 49%)

3. Economic, geographical, political and legal environment

3.1. Economic environment

Lithuania could be described as a small and open economy. The main four economic areas of focus are: shared services (Finance and Accounting, Human Resources, Legal and IT), manufacturing (Mechanical Engineering, Electronics and Lasers), technology (Software Development, IT outsourcing, Data Centers and Game Development); life sciences (Biosimilars, Industrial Biotech and Medical Devices).

In spite of Lithuania's close economic ties with its eastern neighbor, bilateral relations between Lithuania and Russia remain relatively tense. Similar to its Baltic peers, Lithuania opted for strong Euro-Atlantic ties following its independence from the Soviet Union, which is reflected in strong commitment to NATO and European Union membership. In spite of the very deep recession in 2009 and the ensuing strict fiscal consolidation course pursued by the previous and the current government, Lithuania's political and social situation is quite stable. Because of the successful implementation of these policies, Lithuania succeeded in reining in large current account and budget deficits and restored its export competitiveness.

Since 2008 Lithuania has been ranked among the fastest growing economies in the EU. Added to this, Lithuanian can-do-approach has enabled to jump eight places since 2013 for the ease of starting a business to 11th place globally in the World Bank's Doing Business Report[2]. Moreover, Lithuania is a member of European Union and the biggest economy of all Baltic States. 1 January 2015 Lithuania adopted euro and became the 19th member of Euro zone.

GDP per capita in Lithuania is 75% of the EU average of 12,428 EUR. Lithuania has managed to maintain a coherent approach to enhancing fiscal discipline while managing public finances and implementing important updates in key political programs. Despite the presence of internal economical risks and the ever-changing geopolitical situation, growth is expected to remain among the strongest in the Europe, driven above all by internal demand.

Lithuania attracts foreign investors because of its skilled workforce, reliable infrastructure and a larger domestic market than the other two Baltic States. However, Lithuania is dominated by low income levels - the average monthly gross wage is only EUR 699.

There is still a high level of shadow economy, which might make 27% of GDP. With respect to the results of different researches, the scope of shadow economy in Lithuania in 2014 constituted 25-27%

[2] http://www.doingbusiness.org/rankings

(survey data of Lithuanian Free Market Institute indicate 25% of GDP; F. Schneider indicates 27% of GDP).

Lithuania seeks to become an innovation hub by 2020. To reach this goal, it is putting its efforts into attracting FDI to added-value sectors, especially IT services, software development, consulting, finance, and logistics. Well-known international companies such as Microsoft, IBM, Transcom, Barclays, Siemens, SEB, TeliaSonera, Paroc, Philip Morris established a presence in Lithuania.

3.2. Geographical environment

Lithuania is a country in Europe, most populous of the Baltic States (approx. 3 million). Lithuania covers an area of about 65,200 km^2. Lithuania is situated on the eastern shore of the Baltic Sea and borders Latvia on the north, Belarus on the east and south, and Poland and the Kaliningrad region of the Russian Federation on the southwest.

Lithuania's northern neighbor is Latvia. The two countries share a border that extends 610,3 km. Lithuania's eastern border with Belarus is stretching 678,8 km. The border with Poland on the south is relatively short, only 104,3 km. Lithuania also has a 294,4 km. border with the Kaliningrad region of the Russian Federation. Lithuania has 91 km of Baltic seashore with an ice-free harbor at Klaipėda.

3.3. Political and legal system

The Constitution of the Republic of Lithuania was adopted in the Referendum of 25 October 1992 and established the political and legal foundations in Lithuania. The President of Lithuania is the head of state of the country, elected directly for a five-year term and can serve maximum of two terms consecutively. The President, with the approval of the Seimas, is first responsible of appointing the Prime Minister. Upon the Prime Minister's nomination, the President also appoints and dismisses, under the recommendation of the Prime Minister, the Council of Ministers, as well as a number of other top civil servants. The President also serves as the commander-in-chief, oversees foreign and security policy, addresses political problems of foreign and domestic affairs, proclaims state of emergency, considers the laws adopted by the Seimas, and performs other duties specified in the Constitution.

The Seimas has 141 members that are elected for a 4-year term. About half of the members are elected in single-member districts (71), and the other half (70) are elected in the nationwide vote using proportional representation by party lists. A party must receive at least 5% of the national vote to be represented in the Seimas.

Politics of Lithuania takes place in a framework of a parliamentary representative democratic republic, whereby the Prime Minister of Lithuania is the head of government. Executive power is exercised by the President and the Government, which is headed by the Prime Minister. Legislative power is vested in the Seimas (Lithuanian Parliament). Judicial power is vested in judges appointed by the President of Lithuania and the Seimas (the Seimas appoints the judges of the Supreme Court upon submission by the President of the Republic of Lithuania). Court is independent of executive and legislature power and follows the Constitution and laws. The judiciary consists of the 62 courts of general jurisdiction and courts of special jurisdiction.

The Supreme Court of Lithuania (1), the Court of Appeal of Lithuania (1), regional courts (5) and district courts (49) are courts of general jurisdiction dealing with civil and criminal cases. District courts also hear cases of administrative offences coming within their jurisdiction by law. The regional courts, the Court of Appeal, the Supreme Court of Lithuania have the Civil Division and the Criminal Division.

The Supreme Administrative Court of Lithuania (1) and regional administrative courts (5) are courts of special jurisdiction hearing disputes arising from administrative legal relations.

The Constitutional Court of the Republic of Lithuania ensures the supremacy of Constitution within the legal system as well as constitutional justice by deciding whether the laws and other acts of the Seimas are in conflict with the Constitution, and whether the acts of the President of the Republic and the Government are in conflict with the Constitution or laws.

Rulings of the Constitutional Court are promulgated on behalf of the Republic of Lithuania. The decisions of the Constitutional Court on the issues assigned to its competence by the Constitution are final and not subject to appeal. The decisions of the Constitutional Court have the force of a law and are binding on all powers in institutions, courts, all enterprises, institutions and organizations, officials and citizens (erga omnes).

The Prosecution Service of the Republic of Lithuania is a public authority that performs the functions described in the Constitution of the Republic of Lithuania, Prosecution law and other regulation. The Prosecutor's Office is responsible for the arrangement and execution of pre-trial investigations, the public prosecution in criminal cases, the protection of a public interest, likewise ensuring the legality of and assistance to the courts of justice. The Prosecutor's Office is also involved in the preparation and implementation of national and international crime prevention programs, participates in the legislative process, controls the presentation of criminal conduct and their enforcement, coordinates pre-trial investigation institutions in criminal matters, etc.

Public Prosecutor's Office is headed by the Prosecutor General who is appointed and dismissed by the President with the approval of the Seimas every 5 years and cannot be assigned for more than two consecutive terms.

The state police is a major pre-trial investigation institution. As well, the State Border Guard Service, the Special Investigation Service, Military Police, the Financial Crime Investigation Service, the customs authorities of the Republic of Lithuania, the Fire and Rescue Department are the pre-trial investigation institutions, which investigate the criminal acts discovered in the course of their direct functions set out in the laws regulating the activities.

In Lithuania, pre-trial investigations are organized and led by public prosecutors. The prosecutor may himself decide whether to conduct the entire investigation or a part while certain pre-trial investigation actions are carried out by the investigating judge.

Every time when elements of a criminal offence are discovered, the prosecutor and the institutions of pre-trial investigation must, within the limits of their competence, take all measures provided by the law to conduct an investigation, and establish that a criminal act has been committed.

The Lithuanian legal system is principally based on the legal traditions of continental Europe and is grounded on the principles laid out in the Constitution of the Republic of Lithuania and safeguarded by the Constitutional Court of the Republic of Lithuania.

In the Lithuanian legal system, the principal body of law is statutory. Substantive branches of the law are codified in codes. The criminal law is codified in a single legal act - the Criminal Code of the Republic of Lithuania which is in force since 1 May 2003.

The European Union law is an integral part of the Lithuanian legal system since 1 May 2004.

4. Overview of organized crime and TF in Lithuania

4.1. Overview of organized crime in Lithuania

The main areas of the illegal activity of organized criminal groups (further – OCGs) remain the same: illicit drug trafficking, smuggling, economic and financial crimes. Depending on the structure of the groups, the OCG activity can be associated with other crimes, e.g. robbery, theft or extortion. The groups give a great deal of attention to self-protection measures; therefore, they use the most advanced technologies and expand their international connections. The illegal activity of OCGs takes place not only in Eastern Europe countries, but also in other European Union member states and other countries. The members of OCGs aiming to legalize funds acquired by criminal measures tend to invest in legal business: real estate sales, construction of residential premises, various mediation services, freight forwarding companies, involvement in the absorption of the EU structural funds for the agricultural sector, agricultural development and privatization of state-owned land.

Several international and higher level OCGs (according to the EU criteria) operate in the country. Moreover, groups that only partially comply with the characteristics of OCGs and newly forming OCGs are identified in Lithuania.

Geographically, OCGs mostly operate in Kaunas, Panevėžys, Šiauliai and Vilnius districts. In those areas OCGs have been historically the strongest, meeting the criteria of international level OCGs. A continuous monitoring and control of forming groups in every district of the country is performed with the purpose of dissipating them and preventing from growth.

The OCGs operate not only in a specific area of the Republic of Lithuania: the activity of several such groups is carried out in foreign countries too. Some OCG members may be involved in criminal offences, for instance, in Spain or Norway (theft), other members of the same group may organize and execute the distribution of illegal drugs and create networks in Germany and Iceland, others may be forming prostitution networks, producing counterfeit currency and distributing.

Lithuanian tendencies related to organized crime are as follows:

- Sufficient and adequate law enforcement exists in the country to control this phenomenon. There is an unfavorable legislative as well as social environment for the development of organized crime;
- The OCGs are directed towards international crime and avoid publicity, therefore, the violence is usually directed inwards;
- OCGs do not specialize. They are involved in poly-crimes (various types of criminal offenses, searching for the most profitable ones and adapting to new circumstances, e.g. illegal activities in cyberspace);
- Main areas of activity: illicit drug trafficking, smuggling of excise goods, fraud, large-scale theft, settlements in counterfeit money, counterfeit money production and sale are gaining momentum too;
- Lower-level / emerging gangs are more brutal, trying to establish their status in the criminal world by demonstrating force.

4.2. Crime statistics

According to the 2014 data of the Information Technology and Communication Department under the Ministry of the Interior, 4,063 serious and very serious crimes were registered in the country (in 2013 – 4,384 crimes). In the general crime structure, serious and very serious crimes make 4.9 percent of all registered criminal offences, i.e. compared to last year, the percentage of offences in this category slightly decreased – by 0.3 percent.

In 2014, the following serious and very serious crimes were dominant:

- Unlawful possession of narcotics for the purpose of distribution, or possession of their large quantities;
- Serious fraud;
- Smuggling;
- Unlawful possession of excise goods;
- Robbery.

The rate of the following serious and very serious crimes decreased: killings, large-scale theft, robbery, abduction and large-scale smuggling of firearms, ammunition and explosive materials, illegal possession of excise goods.

Number of reported criminal offences during the period 2012-2014 are as follows:

Reported criminal offences			
Criminal Offence	Number of reports in 2012	Number of reports in 2013	Number of reports in 2014
Participation in an organized criminal group and racketeering	34	24	17
Terrorism, including terrorist financing	-	3	3
Trafficking in human beings and migrant smuggling	26	67	75
Sexual exploitation, including sexual exploitation of children	441	321	400
Illicit trafficking in narcotic drugs and psychotropic substances	1664	811	926
Illicit arms trafficking	365	356	543
Illicit trafficking in stolen and other goods	459	432	338
Corruption and bribery	907	1101	809
Fraud	4980	5541	5090
Counterfeiting currency	561	586	496
Counterfeiting and piracy of products	71	90	28
Environmental crime	44	30	36
Murder, grievous bodily injury	356	373	361
Kidnapping, illegal restraint and hostage-taking	61	47	44
Theft	32344	31217	27114
Smuggling	291	560	329
Extortion	159	160	146
Piracy	-	1	2
Robbery	1923	1866	1688

4.3. Overview of TF in Lithuania

No terrorist organizations, groups associated with them or independently operating extremists were identified in Lithuania. There were no direct threats of committing a terrorist act in Lithuania or against

its citizens or objects abroad. According to the assessment of the State Security Department, there is a low threat of a terrorist act in Lithuania. Lithuania formally applies a low level of threat of terrorist attacks, meaning that a terrorist attack is unlikely.

Taking this into consideration, in Lithuania there is a low expectancy level of a potential terrorism financing risk. During the last five years, no foreign terrorist-financing cases were identified in Lithuania. However, it is possible that persons residing in Lithuania, especially coming from countries where terrorist organizations actively operate, can support terrorists abroad using different methods of disguising fund movement.

Newly-emerging tendencies of terrorist threats in the EU and other Western countries show that there are more independently-planned terrorist acts requiring small funds and carried out by individual extremists. Increasingly, terrorist attacks in Europe are arranged by persons using their own resources, having no direct connection and support from terrorist organizations for the execution of their terrorist acts.

5. The stakeholders

The risk assessment assists the stakeholders in determining whether they have weaknesses in their structures, which may impede the system from being compliant to AML/CTF regulations and standards.

The stakeholders are established in accordance with their attributions and responsibilities in the matter of prevention and control of the ML/TF phenomenon. The processes of the NRA are performed in accordance with the profile of the stakeholders, as their activity determine the risk owners with their responsibilities for the management, monitoring and control of the identified risks, including the implementation of the risk responses. The stakeholders will further be required to assess the risks.

5.1. Overview on the Lithuanian ML/TF prevention system

The NRA performed by Deloitte addressed all the possible threats and vulnerabilities of the Lithuanian AML/CTF system, in order to evaluate the compliance with the legal requirements and FATF standards. The Lithuanian AML/CTF system consists of four interconnected components, as follows:

1. The FIU, which is the center of the National AML/CTF system and coordinates the mechanisms and actions for preventing, detecting and controlling the money laundering and terrorism financing criminal activities;
2. The law enforcement and other state authorities;
3. The supervision and regulation authorities;
4. The financial institutions and other entities.

These components are linked to each other in order to provide an effective cooperating workflow, which ensures productivity and coherence in the fight against the crime phenomenon of ML/TF.

5.2. FIU - The Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania

The Financial Crime Investigation Service (hereinafter referred to as “FCIS”) is the main institution, which co-ordinates the implementation of AML/CTP measures in Lithuania. This authority is a law enforcement body, accountable to the Ministry of the Interior of the Republic of Lithuania, and has the ability to receive classified financial information and data provided by financial and designated non-financial institutions that support criminal activities investigations to ensure detection and control of ML/TF. Identifying suspicious transactions, locating assets that may be subject to AML/CTF legislations and supporting prosecution are some of the most relevant responsibilities of FCIS as a FIU.

FCIS' activities regulated in accordance with the Law on the Financial Crime Investigation Service laying down the operating principles, legal framework, objectives and functions operating controls, inter-institutional cooperation framework, powers for attorney for employees, their rights, duties, responsibilities, funding and other issues. FCIS' activities are based on the overall legitimacy, human rights and respect for freedom, equality before the law, likewise openness of activities and confidentiality, personal initiative and official discipline harmonization principles.

FCIS' strategic objective is to improve operating methods by fighting against the criminal activities violating public finance system. This objective could be achieved through criminal intelligence measures such as revealing criminal offenses to the financial system initiating pre-trial investigations, implementing the money laundering and terrorist financing prevention measures, ensuring the surveillance of the European Union (EU) financial interests, performing the expertise of one's commercial and financial activity, conducting the prevention of the criminal acts, affecting the financial system, and enabling to recover the evaded taxes, in order to assure that the operating activity would make a positive impact for the state budget.

The main responsibilities of the FCIS include:

1. Protect the state financial system from criminal influence;

2. Ensure the detection and investigation of any criminal offenses in connection with the funding flows from the European Union or other foreign partners;

3. Uncover and investigate the crimes and other violations of the financial system likewise related crimes and other violations of law;

4. Implement preventive measures against crimes and other violations of the law of the financial system and the related violations of law;

5. Perform other FCIS objectives as it is described by the other legislation.

On 1 December, 2013 the Money Laundering Prevention Board within the FCIS was established in order to implement AML/CTP measures and to perform the following functions:

1. Implementing precautionary measures preventing money laundering and terrorist financing to reveal this type of criminal acts and other violations of law;

2. Collecting and recording information related to money laundering and terrorist financing prevention likewise submitting instructions to the financial institutions and other entities containing feasible solutions for improving money laundering and terrorist financing prevention system;

3. Collecting data about the assets of the particular persona and other related natural and legal persons, transactions and financial operations, asset locations in order to identify the properties that could have been acquired illegally and could be used to ensure the confiscation;

4. Monitoring the activity of different financial institutions and other entities, providing the methodological assistance and information about the criteria for recognition of possible money laundering and/or terrorist financing as well as suspicious monetary operations or transactions; submitting the requirements in order to prevent from the ML/TF.

As a Financial Intelligence Unit, the FCIS ensures an adequate cooperation not only with every national institution, but also with foreign FIUs and international associations, in order to succeed in preventing and controlling the ML/TF phenomenon, in identifying the system's threats and vulnerabilities and applying the most appropriate strategies in this respect.

Under the international regulations this authority must have the ability of receiving and analyze the Suspicious Transaction Report ("STR") and all of the financial information and data that may support criminal investigations. Based on the performed analyzes, FCIS annually releases overviews on the activity of prevention of ML/TF. In addition, the Lithuanian FIU offers support on ML/TF issues to the public and private sectors that fall under the AML/CTF regulations.

5.3. Law Enforcement and other state authorities

The purpose of money laundering is to give the illicit funds the appearance of a legal origin. Because law enforcement and prosecutorial authorities have the abilities of tracing funds and property transfers, their efforts should also be focused on tracing the funds and properties, which are destined to terrorist financing.

These authorities handle criminal intelligence and have an important role in investigating and prosecuting money laundering and terrorist financing.

The following Lithuanian Law Enforcement, prosecutorial and other state authorities have been identified as stakeholders of the NRA:

- Prosecutor's Office;
- Judges;
- Customs Department under the Ministry of Finance of the Republic of Lithuania;
- Police Department;
- Special Investigation Service;
- State Border Guard Service;
- State Tax Inspectorate;
- The State Security Department.

5.4. Regulatory and supervisory authorities

Under the FATF Recommendations, every country establishes AML/CTF regulatory and supervisory authorities, which have the ability of monitoring and supervising the financial institutions and the designated non-financial businesses and professions that fall under the AML/CTF laws and regulations, for overseeing the proper application of AML/CTF legal provisions. In this respect, countries must ensure that their supervision and regulatory activities are performed in an independent and autonomous manner.

The Lithuanian regulatory and supervisory authorities responsible for AML/CTF have been identified as follows:

- The Bank of Lithuania;

- Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania;
- The Lithuanian Bar Association;
- The Chamber of Notaries;
- The Lithuanian Chamber of Auditors;
- The Chamber of Bailiffs;
- The Lithuanian Assay Office;
- The Department of Cultural Heritage Protection under the Ministry of Culture of the Republic of Lithuania.

In conducting supervision activities, the regulatory and supervisory authorities must have access to all relevant information and data on ML/TF risks regarding the customer, the transaction or the business and further report them to the FIU, if there is the case.

In addition, these authorities assess the efficiency and adequacy of the financial institution's and DNFBP's internal controls and monitoring processes. If inconsistencies are found, the regulatory and supervisory authorities impose restrictions and disciplinary or financial sanctions, including the withdrawal or suspension of the business license.

The Bank of Lithuania is included among the most important state institutions. Its principal objective is to maintain price stability. In seeking its principal objective, the Bank of Lithuania is independent from the Government of the Republic of Lithuania or other institutions of the state**.** With Lithuania entering the euro area on 1 January, 2015, the Bank of Lithuania became part of the Eurosystem and together with the European Central Bank (ECB) and the central banks of the other euro area countries will participate in the establishing and implementation of the euro area's monetary policy.

The Bank of Lithuania issues permits and licenses for the financial market participants to operate. The goal of licensing is for the country's financial markets to be operated by reliable, transparent and financially able market participants, while their leaders would be competent and of good repute. The Republic of Lithuania's central bank monitors the financial market players and evaluates their compliance (including AML/CFT issues) with the defined requirements and prudential guidelines, applying sanctions if they violate existing law.

Gambling Control Authority participates in the implementation and development of the gambling related public policies and carries out the gambling supervision. Among the key functions assigned to it, Gambling Control Authority is also responsible for the control of the entities, in order to ensure that the hugest organizers of games of chance and lotteries comply with the laws and regulations' requirements related to the organizing of the gambling and lottery in Lithuania.

Lithuanian Bar Association – self-regulatory institution of advocates, which brings together all lawyers, coordinates their activities in providing legal services to individuals and legal entities, represents their interests and defends them, as well as meets other public interests.

Chamber of Notaries – self-governing body, which assembles 266 notaries working in Lithuania. Major objectives and functions of the Chamber of Notaries: to coordinate the activities of notaries; to take care of the professional development of notaries; to represent the interests of notaries and defend them before the State authorities and the Government institutions; to make the notarial practice more uniform; to exercise control to make sure that notaries adequately perform their duties.

A public legal entity the Lithuanian Chamber of Auditors is unifies all certified auditors of Lithuania, coordinates their activities, represents their interests and meets other public interests. It also carries out regular supervision of auditors and audit companies' activities in Lithuania, is responsible for the registration of companies in the list of Lithuanian audit companies and deletion from it, representation of auditor's interests at the State authorities and the Government institutions of Lithuania etc.

The Chamber of Bailiffs acts under the Law on Bailiffs of the Republic of Lithuania, the Republic of Lithuania Law on Associations and the Charter of the Chamber of Bailiffs. The Chamber of Bailiffs brings together 100 firms, which employ 117 bailiffs. It also coordinates the activities of bailiffs, represents the interests of bailiffs, organizes and carries out the bailiffs and bailiffs' assistants training etc.

The Lithuanian Assay Office perform the testing, analysis, hallmarking, stamping and expertise of different precious metals, gems and their products, as well as determines the characteristics, issues quality certificates and acts of expertise regulations. It also tests the institutions that buy, sell, use, store, process the precious metals, gems, their scrap and waste, or produce the products made from them, and performs other functions assigned by law.

The Department of Cultural Heritage Protection under the Ministry of Culture of the Republic of Lithuania performs the functions of the protection of immovable cultural heritage and movable cultural properties assigned to it by laws and other legal acts; these functions include aid and support or compensation to the cultural heritage managers for its handling; maintenance of accounting and control of cultural heritage as well as presentation of cultural heritage to the society; the Department also contributes to the formation and implementation of national policies in the area of protection of cultural heritage.

All previously mentioned institutions participate in AML/CTF process, as well. By collecting, storing and analyzing information about the controlled entities, they cooperate with FIU and timely inform FIU about possible violations of the legislation, related to the ML/TF.

5.5. Financial Institutions

The following financial institutions have been identified as stakeholders of the national AML/CTF risk assessment:

- Lithuanian commercial banks and branches of foreign banks;
- Intermediary companies on the capital market;
- Life insurance companies;
- Leasing companies not related to commercial banks;
- Money remitters and transfer agents;
- E-money agents;
- Credit unions;
- Quick credit institutions;
- Securities;
- Payment institutions;
- Currency exchange operators;
- Others.

FATF recommends financial institutions to have high professional standards and take prudential measures in order to prevent the risk of committing money laundering or financing of terrorism with the use of their financial products or services.

Financial institutions must develop and implement adequate internal policies and procedures that will include efficient customer due diligence measures, in order to keep the business relationships with their customers transparent. Another obligation for the financial institutions is to periodically evaluate and keep under control the ML/TF risks within the business activity, in accordance with the AML/CTF regulations and best practices. This is not only a legal obligation, but a business partnership requirement also. For example, for banking institutions, being AML/CTF compliant has become a mandatory condition in initiating correspondent banking relationships.

In Lithuania, number of financial entities are the following:

FINANCIAL SECTOR	
Entity	Number
Banks	7
Branches of foreign banks	8
Credit Unions	76
Insurance (overall)	24
Life insurance	9
Securities	31
Payment institutions	37
E-money institutions	3
Currency exchange operators	8

5.6. Designated Non-Financial Businesses and Professions – ("DNFBP")

Due to the nature of the activity they are performing, FATF recommends that some national businesses and professions should have the obligation of applying customer due diligence measures on the client portfolio and the obligation of performing transaction reporting to the Lithuanian FIU.

The AML/CTF requirements for the DNFBPs are not as rigorous as the ones for the financial institutions, but their activity must take prudential measures for not being used as a means for money laundering and terrorism financing, they must conduct ML/TF risk assessments and perform customer due diligence processes that allow the FIU, the supervisory authorities and the law enforcement authorities to adequately identify their customers and trace funds, if necessary.

In Lithuania, number of some non-financial entities is the following:

NON-FINANCIAL SECTOR	
Entity	Number
Casinos	17
Dealers in precious metals and stones	1341

Persons licensed to deal in antiques	71
Lawyers	1989
Notaries	266
Audit firms	174
Bailiffs	118

6. Information on identified ML/TF Risks

81 risks which affect or may affect Lithuania in matter of ML/TF were identified and received scores from 3 to 13, as presented in *Appendix 4 – "List of Lithuanian ML/TF risks"*. Based on risk assessment results, the following response strategies were identified:

1. Mitigation – the response for 39 risks;
2. Avoidance – the response for 13 risks;
3. Sharing – the response for 8 risks;
4. Acceptance – the response for 21 risks.

The response strategies were established as presented in *Appendix 4 – "List of Lithuanian ML/TF risks"*. A risk owner was defined for each identified risk, in accordance with the stakeholders' AML/CTF attributions and responsibilities.

In this respect, the Risk Owners will be responsible for the implement measures to mitigate the ML/TF.

Further in this report high priority risks are described, which received a score above 10 based on the risk scoring matrix. These risks have a high priority in being addressed by the stakeholders.

The risks were divided into four AML/CTF sectors, taking into consideration the Lithuanian AML/CTF system, as follows:

- Law Enforcement Authorities;
- Supervision and Regulatory Sector;
- Financial sector;
- Non-financial sector.

The AML/CTF assessment followed the stages presented in Chapter 2 – "Methodology". In this respect, the information was collected based on documentation review, the stakeholders' responses to AML/CTF questionnaires or the interviews with the representatives of the stakeholders. The risks have been divided into four categories, each related to the sectors of the AML/CTF national system.

Law Enforcement Authorities should have adequate financial, human and technical resources in order to ensure the implementation and the enforcement of the AML/CTF laws and regulations. The identified risks related to the LEAs are mostly caused by insufficient resources, lack of motivation or competence in investigations of crime, which generate substantial proceeds.

Supervisory authorities have the obligation of assessing the compliance of the reporting entities with the AML/CTF requirements and to impose sanctions if they find inconsistencies. In this respect, the Lithuanian financial market is entirely supervised by the Bank of Lithuania, which possesses a high level of AML/CTF knowledge. However, the human resources are extremely short, only 2 persons being

responsible with AML/CTF supervision. This may entail significant difficulties in monitoring the activity of the financial market in terms of AML/CTF.

Financial institutions have a high level of awareness on AML/CTF requirements; the deficiencies are insignificant and can be redressed with practical trainings and workshops. The non-financial sector includes the DNFBPs, named as “other entities” in the Lithuanian AML/CTF Law. With respect to DNFBPs’ nature of business, each of them is supervised by a relevant body. According to the responses to the questionnaires as well as the interview results, some DNFBP sectors lack the knowledge and general understanding of proper identification of their clients and other responsibilities related to the prevention of ML/TF. It is an especially common issue in the gambling sector. The Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania needs to develop AML/CTF supervision programs. The Chamber of Bailiffs and the Lithuanian Bar Association should expand the understanding of their subordinate bodies on their responsibilities in the area of AML/CFT, and systematically verify the application of related regulations in the area.

6.1. Results of the risk assessment

6.1.1. Law Enforcement Authorities

9 high-priority risks were identified, which obtained scores between 10 and 12.

INEFFECTIVE DETECTION, INVESTIGATION AND PROSECUTION OF ML OFFENCE	
Risk Owner:	Prosecution Office
Causal Factors:	This risk was identified based on the statistics provided by the Council of Europe MONEYVAL committee, according to interviews which indicated the lack of ML investigated cases. The low level of ML investigated, prosecuted and convicted cases determine an insufficient level of expertise, as the LEAs do not had the opportunity of practice. Also this risk refers to not being able to get ML/TF convictions due to the obligation of presenting direct evidence of the offence. Generally, the criminals are convicted only for the predicate offences and the ML is not investigated in most of cases. It is important to note, that in 2014 60 ML investigations were carried out and only 4 were final convictions, in 2013 only 1 final conviction was out of 56 investigations carried out. During the interview with law enforcement authorities, it was noted that, in some cases, a relatively small number of predicate offences related to ML are detected and investigated as a result of the lack of competence in collecting information and data about financial aspects of predicate offences; about the financial gain from predicate offences; about disposable assets of individuals and their subsequent use; about what constitutes the essence of asset recovery and what factors predetermine potential ML cases.
Likelihood score:	4
Impact Score:	3
Vulnerability Score:	3

Overall Score	10
Response:	MITIGATION
Recommendation:	LEAs should obtain a high-level awareness and expertise on tracing assets by attending specialized trainings and workshops. The LEAs should change their routines and action plans for investigating ML/TF and could exchange experience with other law enforcement authorities from other countries and jurisdictions. The investigators should participate in workshops, events or brainstorming sessions in order to obtain a clear perspective on how to maximize their work with fewer efforts. An improved amendment of the Penal Code, providing liability for money laundering, should be considered in order to facilitate the substantiation of money laundering activities.

ORGANIZED CRIME INVOLVING PROCCEDS GENERATED BY CRIMES: SMUGGLING OF GOODS, FRAUD AND DRUG TRAFFICKING	
Risk Owner:	LEAs
Causal Factors:	This risk has been identified in the documentation review phase of the NRA and has been later confirmed during interviews with the law enforcement authorities. Even if Lithuania has made significant efforts to minimize this crime phenomenon, it still represents a considerable threat to the AML/CTF system, as it represents one of the most common and menacing predicate offence for ML. Organized crime poses a large problem for LEAs with respect to smuggling, due to its geographical position, being a transit state for smuggling activity[3]. Regarding drug-related offences, the rate of illegal drug use has increased in recent years and has resulted in an increasing number of high-risk crimes[4]. The LEAs representatives informed that they do not have sufficient financial resources in order to timely and fully implement measures requiring immediate action. After the meetings with LEAs it was noted that currently there are no adequate preventive measures and tools to effectively preclude criminal capital interventions into the legal market.
Likelihood score:	5
Impact Score:	4
Vulnerability Score:	3
Overall Score	12
Response:	MITIGATION
Recommendation:	The state budget should allow the LEAs to take the appropriate actions in order to minimize this threat by providing all the necessary means to

3 According to Lithuania 2015 Crime and Safety Report issued by OSAC in May 18, 2015
4 According to Lithuania 2014 Crime and Safety Report issued by OSAC in June 10, 2014

	investigate and to obtain satisfactory results in countering organized crime. LEAs must continue organizing international trainings and workshops for exchanging experience. Adequate preventive measures and tools to effectively preclude criminal capital interventions into the legal market should be developed, i.e. confiscation and extended confiscation of property, transferring the means of litigation burden to the administrative and civil processes. The Customs of the Republic of Lithuania should develop measures in their annual strategic plans to comply with FATF Recommendation No. 32 on Cash Couriers and No. 38 on Mutual Legal Assistance: freezing and confiscation.

FAILURE IN DETECTING TAX EVASION	
Risk Owner:	Tax administrators, LEAs
Causal Factors:	Even though Lithuania has made a significant and continuous progress in combating tax evasion, there is still a high level of shadow economy, which might make 27%[5] of GDP. Tax evasion is a common predicate offence.
Likelihood score:	5
Impact Score:	4
Vulnerability Score:	2
Overall Score	11
Response:	MITIGATION
Recommendation:	The LEAs, tax administrators while focusing on detecting tax evasion, should increase preventing measures as well. In this respect, these institutions should consider taking preventive and suppressing measures, such as: • Increasing the efficiency of applied sanctions; • Increasing the quality of controls, by increasing the professional knowledge of the control teams; • Implementing and/or enhancing controls on electronic commerce; • Enhancing the collaboration and experience changes with EU institutions with similar attributions and responsibilities; • Enhancing controls on goods and cash entering the country.

LOW LEVEL OF EARNINGS OF THE POPULATION	
Risk Owner:	Seimas and Government
Causal Factors:	The low income level (average monthly gross wage is only EUR 699) and economic inequality can entail not only migration, but can also cause an increase of predicate offences and a decrease of trust in the state structures.

[5] Based on the statistics from the AML/CTF questionnaires completed by the Lithuanian State Tax Inspectorate. With respect to the results of different researches, the scope of shadow economy in Lithuania in 2013 constituted 25-32% (survey data of Lithuanian Free Market Institute indicate 25% of GDP; F. Schneider indicates 27% of GDP).

Likelihood score:	5
Impact Score:	1
Vulnerability Score:	5
Overall Score	11
Response:	SHARING
Recommendation:	Due to the improving economic situation in the country, this risk is continually decreasing.

CORRUPTION	
Risk Owner:	Seimas and Government, LEAs and Prosecution Office
Causal Factors:	Corruption is one of the most significant predicate offences, internationally claimed to be generating substantial proceeds of crime. Corruption is caused by the latency of corruption-related criminal offences; lack of transparency; inefficient controls; small penalties; lack of awareness or lack of courage among population to denounce corrupt behavior or other legal violations. Corruption level in Lithuania is still high, however, decreasing tendency is already noticed[6]. In accordance with answers received from the Special Investigation Service to AML/CTF questionnaires, SIS, as opposed to FIU, have fewer measures to operatively obtain information from financial institutions about monetary transactions of private and legal persons. The reason of this is that, in accordance with the Law on the Prevention of ML and TF of the Republic of Lithuania, one of the institutions responsible for the prevention of ML/TF is FIU, and SIS is not included in the list. However, it should be noted that, in accordance with the procedure established by the Government, SIS receives data from FIU on a monthly basis about cash transactions exceeding EUR 15,000.00; therefore, it is possible to conclude that this organization has timely access to comprehensive information about monetary transactions made in the financial and other sectors.
Likelihood score:	4
Impact Score:	4
Vulnerability Score:	3
Overall Score	11
Response:	MITIGATION
Recommendation:	It should be noted that the Decision No. XII-1537 as on 10 March 2015, the Seimas of the Republic of Lithuania established the national anti-corruption program which is a long-term national security enforcement program, the

[6] According to the 2014 data of Corruption Perception Index (CPI), Lithuania was ranked 58 of 100, i.e. 39 of 175 countries participating in the survey. It is the best result of the country since 1999.

	content and scope of which is attributable to the long-term anti-corruption strategy. The purpose of the program is ensuring long-term, effective and targeted corruption investigation, prevention and control system in the Republic of Lithuania for the period of 2015-2025. Lithuania's main objectives (which should be accomplished in a limited period of time) should take into consideration preventing corruption in public institutions, raising the population's awareness, enhancing the administrative and punitive sanctions.

FRAUD	
Risk Owner:	LEAs and Prosecution Office
Causal Factors:	Tax fraud represents an active threat on the Lithuanian financial system, based on the level[7] of shadow economy and on the stakeholders' responses to the NRA questionnaires. Tax fraud means cases when false information or falsification of documents is provided/performed intentionally. Tax evasion means unlawful actions when the obligation to pay taxes is covered up or ignored, i.e. a taxpayer, having covered up income or information from a tax administrator, pays less in taxes than legally obliged.
Likelihood score:	4
Impact Score:	4
Vulnerability Score:	3
Overall Score	11
Response:	MITIGATION
Recommendation:	The law enforcement authorities should develop and implement an action plan, in accordance with the anti-fraud policy of the European Commission[8].

"LONE WOLF" TERRORISM TREND	
Risk Owner:	Law Enforcement Authorities, FIU, FIs and DNFBPs
Causal Factors:	Due to "lone wolf" tactics and actions, law enforcement institutions face serious difficulty to identify such persons, as the identification process requires significant technical, human and time resources.
Likelihood score:	1
Impact Score:	5

[7] Based on the statistics from the AML/CTF questionnaires completed by the Lithuanian State Tax Inspectorate under the Ministry of Finance

[8] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282014%290474_/com_com%282014%290474_en.pdf

Vulnerability Score:	4
Overall Score	10
Response:	MITIGATION
Recommendation:	The law enforcement authorities should continue on attending trainings and presentations on “lone wolf” terrorism and terrorism trends. In addition, law enforcement authorities must take into consideration tracking assets and preemptive attacks.

UNTRANSPARENT FUNDING OF POLITICAL CAMPAIGNS	
Risk Owner:	Central Electoral Commission
Causal Factors:	This risk has been identified in the documentation review phase and while conducting the interviews and relates to fraud committed with NPOs that sponsor political campaigns in low transparency conditions.
Likelihood score:	3
Impact Score:	4
Vulnerability Score:	4
Overall Score	11
Response:	MITIGATION
Recommendation:	The Central Electoral Commission must ensure that NPOs reported any sponsorship deals and their purpose. Moreover, law enforcement institutions ought to perform targeted inspections of NPOs more frequently.

PRESENCE OF INDIVIDUALS, GROUPS OR ORGANIZATIONS THAT FINANCIALLY SUPPORT OR PROMOTE VIOLENT EXTREMISM	
Risk Owner:	Ministry of Foreign Affairs, FIU, Law Enforcement and Prosecution Office
Causal Factors:	This risk is caused by the following factors: • current situation in Ukraine and intensified pro-Russian forces directed against NATO and the EU; • illegal migration from African countries to the EU member states. This factor increases the risk of terrorists from Syria and Iraq illegally crossing the EU border; • online propaganda of terrorism and violent extremism; • support for Lithuania from the EU, the UN, NATO and the US executive policy in the area of combating terrorism and violent extremism; • upsurge in the activities of the representatives of several Russian Federation peoples of the dominant Islamic faith (Chechnya, Ingushetia, Dagestan); the potential relations of such persons with Syria, Islamic states and Ukraine, promoting radical Islam, recruiting Islam fighters and pushing to become Shahids (suicide bombers).
Likelihood score:	1
Impact Score:	4
Vulnerability Score:	5

Overall Score	10
Response:	MITIGATION
Recommendation:	The FIU must raise awareness in the reporting entities (financial institutions and DNFBPs) to monitor not only the transactions and customers that present suspicions of ML, but also to constantly verify the targeted financial sanctions. The monitoring activities must not be performed solely by the LEAs, but also by the reporting entities.

6.1.2. Supervision and Regulatory Sector

5 high-priority risks were identified, which received scores between 10 and 13.

INSUFFICENT RESOURCES OF AML/CTF SUPERVISORY BODIES AND/OR INSUFFICIENT AML/CTF SUPERVISION ACTIVITIES	
Risk Owner:	Supervisory Authorities and FIU
Causal Factors:	Inadequate/inefficient supervision is caused by the lack of staffing; lack of IT and financial resources for deploying effective controls on the reporting entities and for ensuring a reporting platform between the reporting entities and the supervisory authorities; inadequate AML/CTF supervising techniques and methods, i.e.: • The Bank of Lithuania: ○ covers the entire financial sector as a supervisory authority with only two employees; therefore, the Bank is very short on human resources with respect to AML/CTF activities. As a result, it may have a negative impact on the efficiency of the supervision of the financial institutions (e.g. the number of trainings, inspections etc.); ○ has no separate inspection methodologies for different categories of financial institutions (currently, there is a general methodology for all financial institutions); ○ performing offsite supervision, the Bank has no specialized tools for supporting the ML/TF risk assessment (for the documentary monitoring, tools for general prudential supervision of financial institutions are used); • Lithuanian Chamber of Auditors, the Chamber of Bailiffs and the Gaming Control Authority have no information systems enabling to collect and analyze data and information provided by supervised entities for the purpose of AML/CTF supervision; • regarding the Gaming Control Authority, it was noted that they do not have any tools for performing AML/CTF risk assessments, no IT application to support the supervision activities and no written instructions on how to perform an AML/CTF inspection; • most of the DNFBPs do not verify the list of targeted financial and other international sanctions issued by the UN or the EU, when initiating or continuing a business relationship with a customer. Also, based on the answers to the NRA questionnaires, reporting entities do not always properly implement the requirements of AML/CTF measures; however, during 2012-2013 supervisory authorities have not identified such non-compliance: • some leasing undertakings do not apply a risk-based approach; • some life insurance undertakings do not collect information related to

	domestic or international PEPs; • DNFBPs do not apply a risk-based approach, do not properly apply the requirements of know-your-client and business relationship monitoring, which results in very few or no STRs received from DNFBPs; • very few or no trainings/consultative meetings organized for bailiffs, casinos, real estate undertakings, audit firms/accountants/tax consultants.
Likelihood score:	5
Impact Score:	4
Vulnerability Score:	4
Overall Score	13
Response:	MITIGATION
Recommendation:	Supervisory authorities must have adequate tools in place for the supervision of ML/TF prevention (both documentary analysis and onsite inspections). DNFBPs' supervisory authorities should adjust their budget in order to allocate enough resources for AML/CTF, including appropriate human and IT resources. In addition, supervisory authorities should establish clear AML/CTF action plans for conducting controls on the reporting entities, in accordance with FATF guidelines. With respect to international sanctions, DNFBPs' supervisory authorities should include in their control programs inspecting whether reporting entities verify their customers in an updated list of designated persons under the EU and the UN sanctions (and OFAC, if applicable), in order to support the reporting entities in applying the targeted financial sanctions and other international sanctions. The budget for each AML/CTF supervisory authority must be adequately allocated in order to ensure appropriate supervision of reporting entities. Having a special position in the supervision of financial institutions, the Bank of Lithuania must immediately solve the issue of the shortage in human resources related to AML/CTF and to make AML/CTF activities a priority area. Supervisory authorities must regularly participate in specialized trainings.

HIGH LEVEL OF CASH TRANSACTIONS	
Risk Owner:	Supervisory Authorities and FIU
Causal Factors:	Large scope of cash transactions potentially increases the scope of tax evasion and the level of shadow economy.
Likelihood score:	5
Impact Score:	3
Vulnerability Score:	5
Overall Score	13
Response:	MITIGATION
Recommendation:	The supervisory authorities must ensure that the reporting entities take prudential due diligence and reporting measures in order to keep an acceptable level of transparency of their customers' transactions and for obtaining a clear understanding on the purpose of the transactional activity. The supervisory authorities must ensure that the reporting entities meet the requirements of identifying the parties of the transaction, the beneficial owner of funds when performing cash transactions. In addition, when performing the STR analysis or when investigating other allegations, the FIU should continue using CTRs information and perform sufficient analytics in order to obtain maximized results on their analysis.

FAILURE TO IMPOSE ADEQUATE SANCTIONS	
Risk Owner:	FIU and Supervisory Authorities
Causal Factors:	In accordance with the interviews and responses received to the AML/CTF questionnaires, insufficient inspections and sanctions were placed for AML/CTF deficiencies. When interviewing and analyzing the questionnaire responses of the participants of AML/CTF system, it was noted that some reporting entities do not comply with AML/CTF legal requirements and still have not been imposed adequate sanctions or have not been inspected by supervisory authorities. For example, reporting entities which responded to the AML/CTF questionnaires that they have not received any sanctions during 2012-2013 (even if, during the interviews and analyzing the other responses to the questionnaires, it was noted that they did not apply all AML/CTF requirements) were the following: • bailiffs (no inspections performed); • casinos (no inspections performed); • notaries (no inspections performed); • audit firms/accountants/tax consultants (no inspections performed). None of the supervisory authorities, with the exception of the Bank of Lithuania, have authority to impose sanctions.
Likelihood score:	4
Impact Score:	4
Vulnerability Score:	4

Overall Score	12
Response:	MITIGATION
Recommendation:	FATF recommends supervisory authorities to apply "effective, proportionate, and dissuasive sanctions" for failure to comply with AML/CFT requirements. The sanctioning regime must increase the level of AML/CTF commitment of the reporting entities. Adequate sanctions should be especially applied to DNFBPs as currently, this reporting category is not sanctioned or insufficiently sanctioned[9].

NO SECTORIAL ML/TF RISK ASSESSMENT CONDUCTED BY THE AUTHORITIES	
Risk Owner:	Supervisory Authorities
Causal Factors:	Lithuania has a low level of awareness[10] on the size of ML/TF risks and vulnerabilities of the national AML/CTF system. The sectorial vulnerabilities and threats related to ML/TF have not been assessed by the supervisory authorities in order to develop adequate action plans for responding to those ML/TF threats and vulnerabilities.
Likelihood score:	4
Impact Score:	3
Vulnerability Score:	4
Overall Score	11
Response:	MITIGATION
Recommendation:	Supervisory authorities must perform a sector-based ML/TF risk assessment with the purpose of identifying risks characteristic to a specific sector. The results of these AML/CTF risk assessments should be submitted to the FIU and then organize workshops and meetings for developing effective action plans for minimizing the sectorial risks. In addition, the FIU should share their insights with authorities that the latter could use information received in their risk assessments.

LIMITED REGULATION OF MONEY OR VALUE TRANSFER SYSTEMS	
Risk Owner:	FIU, Supervisory Authorities
Causal Factors:	Although banking institutions have implemented strict AML/CTF regulations, there is a possibility to avoid the required transparency in cases of cash remittances when a client's funds/assets are being transferred (e.g. no ultimate beneficiary is identified). There is an obvious shortage of detecting cases when a person makes several cash transactions during a certain period

[9] This statement is based on statistics from the NRA questionnaires.

10 Based on interviews held with stakeholders and on the answers received to NRA questionnaires

	of time and their identity remains unknown. A significant part of cash remittance services is provided by foreign financial institutions working through mediators that are not included in the list of entities obliged to comply with the requirements of ML/TF prevention in the Republic of Lithuania.
Likelihood score:	3
Impact Score:	3
Vulnerability Score:	4
Overall Score	10
Response:	MITIGATION
Recommendation:	Foreign financial institutions providing cash remittance services in Lithuania via mediators should be included in the list of entities obliged to comply with the requirements of ML/TF prevention in the Republic of Lithuania. Supervisory authorities must organize regular trainings encompassing the following areas: • identifying a customer and legal/natural persons related (ultimate beneficiaries, other shareholders, administrators, legal representatives); • verifying the information provided by the customer based on internal and external credible sources; • adequately monitoring transactions and collecting a complete set of information regarding the payer/beneficiary of a certain transaction; • collecting information regarding the source of funds, reason for the business relationship and collecting supporting documentation, when applicable; • verifying the payer/beneficiary in updated lists of targeted financial sanctions. Financial institutions providing cash remittance services are recommended to implement IT systems enabling the identification of regular clients, monitoring performed transactions.

6.1.3. Financial Sector

While performing the NRA a large number of high-priority risks in the financial sector were not identified, but the supervisory authorities and LEAs should take special caution on financial institutions, other than banking institutions, taking into consideration that the micro-launderers and the terrorists do not use significantly valuable assets for their criminal purposes.

1 high-priority risk was identified, which obtained scores of 10.

INCREASE USE OF TECHNOLOGY IN MONEY TRANSFER	
Risk Owner:	Financial Institutions and Supervisory Institutions
Causal Factors:	Information technologies in the financial sector are under rapid and continuous development and thus simplify the transaction of funds. Every technological improvement potentially influences the security of information systems and the changes of business processes.

	Financial institutions that adhere to such technological developments (implement or update them) must ensure a high level of IT security.
Likelihood score:	5
Impact Score:	3
Vulnerability Score:	2
Overall Score	10
Response:	MITIGATION
Recommendation:	Financial institutions must conduct risk assessments before implementing new information systems. In addition, financial institutions must conduct IT audits in order to ensure the efficiency of IT systems, the traceability of client transactions and appropriate transparency.

6.1.4. Non-Financial Sector

In this respect, 6 high-priority risks were identified, with scores between 10 and 13.

LACK OF AML/CTF AWARENESS	
Risk Owner:	DNFBPs and Supervisory Authorities
Causal Factors:	Even though banking institutions implemented adequate AML/CTF rules and regulations, DNFBPs have shown a low level of awareness on AML/CTF requirements and risks, due to lack of trainings on practical AML/CTF procedures and processes, i.e. specific situations that the stakeholders may encounter while performing their activity. For example, based on held interviews with the reporting entities (DNFBPs), it was noted that there are cases when the customer identification process is confused with the process of verifying the information provided by the customer using credible external or internal sources of information. In addition, it was encountered that the reporting entities have problems in identifying and verifying the beneficial owner of a company with chained ownership or with ownership in foreign countries, especially tax or secrecy havens. In this case, due to inadequate customer identification and verification of provided information, the reporting entities may apply inadequate customer due diligence measures for the RBA purposes. This problem (of not properly identifying and verifying the Beneficial Owner of company with chained ownership or with foreign ownership) has been encountered in most of the countries that apply AML/CTF requirements.
Likelihood score:	3
Impact Score:	4
Vulnerability Score:	3
Overall Score	10
Response:	MITIGATION
Recommendation:	DNFBPs must conduct specialized AML/CTF trainings for their employees, especially for the ones that have direct contact with the customers and their transactions. Regarding the identification and verification of the Beneficial Owner of companies, the FIU and the Supervisory Authorities of DNFBPs should organize training sessions and workshops in order to ensure that the reporting entities have the adequate knowledge on how to act in situations of customers – companies with chained ownership or foreign ownership (especially concerning tax or secrecy havens), in order to mitigate the risk of not applying the adequate customer due diligence measures due to misleading or insufficient information. For example, in such cases, the reporting entities may use sources of information such as authorized statements from lawyers, audit firms or Trade Register Offices in order to verify the information provided by the customer with respect to its ownership.

INABILITY TO MONITOR TRANSACTIONS

Risk Owner:	DNFBPs and Supervisory Institutions
Causal Factors:	Adequate monitoring activities of the DNFBPs for AML/CTF purposes were not identified and no IT systems or applications noted in this respect. The transactions performed by the DNFBPs' customers are only monitored for accounting purposes, but no internal database was identified, that may support AML/CTF activities, no IT application that monitors the customer/transactions ML/TF risks (at least Customer Relationship Management system). In addition, the DNFBPs are not provided with updated lists of targeted financial sanctions imposed by the EU or UN.
Likelihood score:	4
Impact Score:	4
Vulnerability Score:	5
Overall Score	13
Response:	MITIGATION
Recommendation:	The DNFBPs should ensure an adequate monitoring activity, supported by IT systems or applications, developed in-house or offered by external providers, in order to ensure transparency on the asset transactional activity of their customers. If the DNFBPs cannot afford an AML/CTF IT system or application, the activities must be performed manually, by consulting the EU and UN sanctions, both in terms of international sanctions and targeted financial sanctions. In addition, in order to mitigate the risks that may arise concerning high-risk customer or transaction, the DNFBPs should develop AML/CTF questionnaires to be filled in when entering a business relationship with a customer, in order to understand the risk that the customer exposes the DNFBP. In this respect, if the risk level is higher than normal, enhanced due diligence measures are ought to be taken when performing a transaction for that customer. The DNFBPs should also periodically update a the list of countries considered uncooperative or insufficiently cooperative with respect to AML/CTF and take adequate measures in order to respond to the risks arisen from conducting transactions with these countries.
LACK OF AWARENESS ON ML/TF RISKS AND INABILITY TO APPLY AN EFFECTIVE RISK-BASED APPROACH	
Risk Owner:	DNFBPs and Supervisory Institutions
Causal Factors:	Most of the DNFBPs do not apply a RBA on their customers and show a low level of awareness on AML/CTF risks regarding high-customers, such as risks involving entities or individuals designated in the international sanctions lists, citizens of high-risk countries, entities that perform high-risk activities, entities or individuals that have been investigated for crimes related to ML/TF and

	others. Most of the DNFBPs show a low level of awareness on the exposure of their business to ML/TF risks[11]. The DNFBPs have a low level of awareness on ML/TF risks concerning customers and countries that are considered of high risk, in accordance with AML/CTF standards. They do not apply enhanced due diligence measures in this type of business relationships.
Likelihood score:	4
Impact Score:	3
Vulnerability Score:	5
Overall Score	12
Response:	MITIGATION
Recommendation:	The RBA relates to identifying the risk to which the customer or the transaction exposes the business/profession. In this respect, DNFBPs must implement internal policies and procedures that provide instructions on how to categorize a specific customer/transaction using risk criteria, such as: origin/residence of the customer, origin/destination of funds, activity of the customer, identity of the beneficial owner, international sanctions/targeted financial sanctions and other criteria recommended by FATF or which the business/profession considers to pose a threat to the integrity or reputation. DNFBPs must conduct periodical AML/CTF risks assessments and implement risk response strategies in order to minimize ML/TF threats and vulnerabilities. For this purpose, the DNFBPs must attend specialized trainings and further organize trainings and workshops for the employees.

INADEQUATE IDENTIFICATION OF THE BENEFICIAL OWNER	
Risk Owner:	DNFBPs and Supervisory Institutions
Causal Factors:	Most of the DNFBPs did not implement the obligation of identifying and verifying the Beneficial Owner of their customer and do not follow the FATF recommendations on performing adequate customer due diligence processes. The DNFBPs were unable to identify the Beneficial Owner of complex structures of legal entities, nor of foreign entities.
Likelihood score:	4
Impact Score:	3
Vulnerability Score:	5
Overall Score	12

11 Based on interviews held with DNFBPs' representatives and on the answers received from the DNFBPs to AML/CTF questionnaires.

Response:	MITIGATION
Recommendation:	The DNFBPs should implement in their AML/CTF policies and procedures the obligation of identifying the Beneficial Owner of legal entities and of natural persons that conduct transactions for another person, by requesting the customer to complete a declaration of the Beneficial Owner and, if the case, to provide identification documents, when entering a new business relationship and when conducting occasional transactions that exceed the amount of EUR 15000, whether the transaction is conducted in one or more operations that seem to be linked to each other. In this respect, the DNFBPs must have adequate knowledge on how to identify the Beneficial Owner, in order to be able to explain to the customers what information they are requesting from them. This knowledge is obtained from the FATF Recommendations or by attending specialized trainings and workshops. If it is possible, the DNFBPs should be encouraged to develop in-house AML/CTF databases or purchase programs such as World-Check, Factiva, LexisNexis and other.

LACK OF COMMITMENT OF NON-FINANCIAL SECTOR, INCLUDING LOW LEVELS OF REPORTING AND/OR LACK OF QUALITY OF STRS	
Risk Owner:	DNFBPs and Supervisory Institutions
Causal Factors:	A low level of commitment of the non-financial sector was noted in respect to AML/CTF requirements and reporting of suspicions, due to lack of reports submitted to the FIU.
Likelihood score:	4
Impact Score:	3
Vulnerability Score:	4
Overall Score	11
Response:	MITIGATION
Recommendation:	The DNFBPs must obtain the understanding that the reporting of suspicions and conducting a close collaboration with the FIU and their supervisory authorities reduces the exposure of ML/TF risks. In this respect, the DNFBPs must contact these authorities for every uncertainty in order to conduct a proactive AML/CTF activity.

FAILURE TO VERIFY THE INFORMATION PROVIDED BY THE CUSTOMER	
Risk Owner:	DNFBPs and Supervisory Institutions
Causal Factors:	DNFBPs do not verify the information provided by the customer for AML/CTF purposes when identifying the customer or when performing asset transactions for the customer, especially in case of non-face-to-face business relationships
Likelihood score:	4
Impact Score:	2
Vulnerability Score:	4
Overall Score	10
Response:	SHARING
Recommendation:	In cases of non-face-to-face business relationships, the information concerning the identification of the customer or the asset transaction must be verified using third parties, which may facilitate the customer due diligence processes. In addition, the DNFBPs should request the documentation needed in order to confirm the information provided by the customer, especially concerning the identity of the Beneficial Owner.

6.1.5. Low-priority risks

The identified ML/TF risks that obtained a low score of 3 and 4, have been ranked as low-priority risks and introduced in the Low Risk Watch List, as presented in Appendix 5 – “Low Risk Watch List”.

For these risks Acceptance strategy is as risk response. In these cases, stakeholders are not obliged to build a contingency plan in order to assure the AML/CTF System for the possibility of those risks to occur.

Appendix 1 – Credible Sources

We used the following credible sources for the purpose of our assessment:

1. The responses of the stakeholders to NRA questionnaire
2. Discussions with the stakeholders with which we held interviews
3. National regulations and other legal acts
4. Moneyval reports:
    - *Moneyval's Report on Forth Assessment Visit on Lithuania on 5th of December, 2012*
    - *Moneyval's Executive Summary of the Report on Forth Assessment Visit on Lithuania on 5th of December, 2012*
    - *Moneyval's 2nd Compliance Report on Lithuania issued on 19th of September, 2014*
5. Other reports:
    - *Sustainable Governance Indicators – Report 2014*[12]
    - *The State Security Department of the Republic of Lithuania Annual Threat Assessment 2013*[13]
    - *EUROPOL SOCTA 2013*[14]
    - *EUROJUST Annual Report 2013*[15]
    - *Risk Assessment Improvement in the Investment Project Management: Verbal Analysis Methods*[16]
6. Other sources:
    - *OSAC website*[17]
    - *International Organization for Migration website*[18]
    - *Reuters website*[19]

12 http://www.google.bg/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=10&ved=0CGwQFjAJ&url=http%3A%2F%2Fwww.sgi-network.org%2Fdocs%2F2014%2Fcountry%2FSGI2014_Lithuania.pdf&ei=DjEgVJmUOcTgavPDgbgN&usg=AFQjCNFDdxxMEqvUcLIWaVumJgFpnoOWIg
13 http://www.vsd.lt/Files/Documents/635448351234307500.pdf
14 https://www.europol.europa.eu/sites/default/files/publications/socta2013.pdf
15http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202013/Annual-Report-2013-EN.pdf
16 http://www.ue.katowice.pl/uploads/media/4_G.Shevchenko_L.Ustinovichius_Risk_Assessment....pdf
17 https://www.osac.gov/pages/ContentReportDetails.aspx?cid=15805
18 https://www.iom.int/cms/en/sites/iom/home/where-we-work/europa/european-economic-area/lithuania.html
19 http://af.reuters.com

- *BBC website*[20]
- *Bloomberg website*[21]
- *Transparency International website*[22]
- *Delfi by the Lithuanian Tribune website*[23]
- *Kurier website*[24]
- *Global Edge website*[25]
- *Coface website*[26]

20 http://www.bbc.com
21 http://www.bloomberg.com
22 http://www.transparency.org
23 http://en.delfi.lt
24 http://www.kurier.lt
25 http://globaledge.msu.edu/countries/lithuania
26 http://www.coface.com/Economic-Studies-and-Country-Risks/Lithuania

Appendix 2 – Interviews with the stakeholders

We invited all the NRA stakeholders for discussions. We held interviews with the following stakeholders:

- The Financial Crime Investigation Service under the Ministry of Interior of the Republic of Lithuania
- Supreme Court of Lithuania
- Prosecutor's Office
- National Bank of Lithuania
- The Department of Cultural Heritage Protection under the Ministry of Culture of the Republic of Lithuania
- Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania
- The Lithuanian Bar Association
- The Chamber of Notaries
- The Lithuanian Assay Office
- The Special Investigation Service
- Police Department
- Customs department under the Ministry of Finance of the Republic of Lithuania
- State Border Guard Service under the Ministry of Interior of the Republic of Lithuania
- Auditors
- Banks
- Credit unions
- Pension funds
- Lithuanian bank association
- Lawyers
- Insurance undertakings
- Casinos

Appendix 3 – Questionnaires from stakeholders

Questionnaires for all stakeholders of the NRA were developed and included requests for expert's opinion and for statistics.

The stakeholders who responses were used for the purpose of assessment are as follows:

1. Law Enforcement and other Authorities:
    - FIU
    - Prosecutor's Office
    - Police Department under the Ministry of Interior
    - State Tax Inspectorate
    - Special Investigation Service
    - National Court Administration
    - Criminal Customs Service
    - Customs Department under the Ministry of Finance of the Republic of Lithuania

2. Supervisory and Regulatory Authorities:
    - National Bank of Lithuania
    - Lithuanian Assay Office
    - Lithuanian Bar Association

3. Financial institutions as reporting entities:
    - Banking institutions
    - Life insurance undertakings
    - Leasing undertakings
    - Credit unions

4. Non-financial Businesses and Professions as reporting entities:
    - Audit firms
    - Car dealers
    - Bailiffs
    - Casinos
    - Notaries
    - Real estate undertakings
    - Accountants
    - Tax consultants
    - Lithuanian post office

Appendix 4 – List of Lithuanian ML/TF risks

No.	Owner	RISK ASSESSMENT					STAKEHOLDER RESPONSE
		Risk	Likelihood	Impact	Vulnerability	TOTAL	
1	*Supervisory Authorities, FIU*	*Insufficient resources of AML/CTF supervisory bodies and/or insufficient AML/CTF supervision activities*	*5*	*4*	*4*	*13*	**Mitigation**
2	*DNFBPs*	*Inability to monitor transactions*	*4*	*4*	*5*	*13*	**Mitigation**
3	*Supervisory Authorities, FIU*	*High level of cash transactions*	*5*	*3*	*5*	*13*	**Mitigation**
4	*Law Enforcement Authorities*	*Organized crime involving proceeds generated by crime: drug trafficking, fraud and smuggling of good*	*5*	*4*	*3*	*12*	**Mitigation**
5	*FIU and Supervisory Authorities*	*Failure to impose adequate sanctions*	*4*	*4*	*4*	*12*	**Mitigation**
6	*DNFBPs and Supervisory Authorities*	*Lack of awareness on ML/TF risks and inability to apply an effective risk based approach*	*4*	*3*	*5*	*12*	**Mitigation**
7	*DNFBPs*	*Inadequate verification of the Beneficial Owner*	*4*	*3*	*5*	*12*	**Mitigation**
8	*FIU, State Tax Inspectorate, LEAs*	*Tax evasion*	*5*	*4*	*2*	*11*	**Mitigation**
9	*Law Enforcement Authorities*	*Fraud*	*4*	*4*	*3*	*11*	**Mitigation**
10	*Government and Seimas*	*Low level of earnings of the population*	*5*	*1*	*5*	*11*	**Share**
11	*Supervisory Authorities*	*No sectorial ML/TF risk assessment conducted by the authorities*	*4*	*3*	*4*	*11*	**Mitigation**

No.	Owner	RISK ASSESSMENT					STAKEHOLDER RESPONSE
		Risk	Likelihood	Impact	Vulnerability	TOTAL	
12	*DNFBPs*	*Lack of commitment of non-financial sector, including low levels of reporting and/or lack of quality of STRs*	*4*	*3*	*4*	*11*	**Mitigation**
13	*FIU, Law Enforcement Authorities*	*Untransparent funding of political campaigns*	*3*	*4*	*4*	*11*	**Mitigation**
14	*Government, FIU, Law Enforcement and Prosecutorial Authorities*	*Corruption*	*4*	*4*	*3*	*11*	**Mitigation**
15	*Prosecutorial Authorities*	*Ineffective detection, investigation and prosecution of ML offence*	*4*	*3*	*3*	*10*	**Mitigation**
16	*Financial institutions*	*Increase use of technology in money transfer*	*5*	*3*	*2*	*10*	**Mitigation**
17	*DNFBPs*	*Failure to verify the information provided by the customer*	*4*	*2*	*4*	*10*	**Mitigation**
18	*FIU, Supervisory Authorities*	*Limited regulation of money or value transfer systems*	*3*	*3*	*4*	*10*	**Mitigation**
19	*FIU, Supervisory Authorities, Financial institutions and DNFBPs*	*Lack of awareness on AML/CTF*	*3*	*4*	*3*	*10*	**Mitigation**
20	*FIU, Law Enforcement and Prosecutorial Authorities*	*Presence of individuals, groups or organizations that financially support or promote violent extremism*	*1*	*4*	*5*	*10*	**Mitigation**
21	*FIU, Law Enforcement Authorities, Financial institutions and DNFBPs*	*"Lone wolf" terrorism trend*	*1*	*5*	*4*	*10*	**Mitigation**
22	*Government and Seimas*	*ML/TF inadequately criminalized*	*2*	*4*	*4*	*10*	**Mitigation**
23	*Law Enforcement Authorities*	*No regular reviews of terrorism financing risk in its NPO sector*	*4*	*3*	*2*	*9*	**Mitigation**

No.	Owner	RISK ASSESSMENT					STAKEHOLDER RESPONSE
		Risk	Likelihood	Impact	Vulnerability	TOTAL	
24	*DNFBPs*	*Inadequate due-diligence on prospective customers/third parties*	*3*	*3*	*3*	*9*	**Mitigation**
25	*Government, Financial institutions and DNFBPs*	*Presence of NPOs active in overseas conflict zones or in countries or regions known to have a concentration of terrorist activity*	*1*	*4*	*4*	*9*	**Mitigation**
26	*FIU, Law Enforcement Authorities, Financial institutions and DNFBPs*	*Presence of NPOs raising funds for recipients in a third country which are part of an organizational structure that engages in violent or paramilitary activities*	*1*	*4*	*4*	*9*	**Mitigation**
27	*Law Enforcement Authorities*	*Illegal logging*	*1*	*3*	*5*	*9*	**Mitigation**
28	*FIU, Government and Seimas*	*Failure to define clear strategy on AML/CTF*	*3*	*4*	*2*	*9*	**Mitigation**
29	*Government and Seimas*	*Weaknesses in legislation for combating organized crime*	*3*	*3*	*3*	*9*	**Mitigation**
30	*FIU*	*Lack of early warning arrangements with other FIUs*	*2*	*4*	*3*	*9*	**Mitigation**
31	*Supervisory Authorities, Financial institutions*	*Larger number of offshore accounts*	*3*	*2*	*4*	*9*	**Share**
32	*Supervisory Authorities*	*Failure to train specific units on compliance policies and procedures*	*3*	*2*	*4*	*9*	**Share**
33	*FIU, Law Enforcement Authorities*	*Illicit manufacturing of and trafficking in firearms and their parts*	*1*	*5*	*3*	*9*	**Mitigation**
34	*FIU, Law Enforcement Authorities*	*Raising funds for the purpose of Terrorism or Terrorism Financing*	*2*	*4*	*3*	*9*	**Mitigation**
35	*Law Enforcement Authorities*	*Weak cash courier control at border points*	*4*	*2*	*2*	*8*	**Accept**
36	*Financial institutions*	*Inadequate due-diligence on prospective customers/third parties*	*2*	*3*	*3*	*8*	**Mitigation**
37	*Supervisory Authorities*	*Ineffective supervision and control activities due to insufficient processes and procedures*	*2*	*3*	*3*	*8*	**Mitigation**

No.	Owner	RISK ASSESSMENT					STAKEHOLDER RESPONSE
		Risk	Likelihood	Impact	Vulnerability	TOTAL	
38	*Financial institutions*	*Lack of commitment of financial sector, including low levels of reporting and/or lack of quality of STRs*	*2*	*3*	*3*	*8*	**Mitigation**
39	*Financial institutions*	*Inability to monitor transactions*	*2*	*4*	*2*	*8*	**Avoid**
40	*Financial institutions*	*Failure to verify a foreign Beneficial Owner of a company with chain ownership*	*2*	*3*	*3*	*8*	**Mitigation**
41	*Law Enforcement Authorities*	*Failure to use financial information in investigation*	*2*	*3*	*3*	*8*	**Mitigation**
42	*Financial institutions*	*Inability to identify high AML/CTF risk customers*	*2*	*3*	*2*	*7*	**Avoid**
43	*Financial institutions*	*Existence of high-risk correspondent relationships between banks*	*2*	*3*	*2*	*7*	**Avoid**
44	*Financial institutions*	*High-risk types and ranges of customers*	*2*	*3*	*2*	*7*	**Avoid**
45	*Financial institutions*	*High-risk nature of business relationships*	*2*	*3*	*2*	*7*	**Avoid**
46	*Financial institutions*	*Business and customer base in high-risk geographic areas*	*2*	*3*	*2*	*7*	**Avoid**
47	*Financial institutions*	*High level non-residents*	*2*	*3*	*2*	*7*	**Avoid**
48	*Financial institutions*	*High level of trans-national movements of funds*	*2*	*3*	*2*	*7*	**Avoid**
49	*FIU and Supervisory Authorities*	*Lack of practical AML/CTF guidance and compliance programs for the reporting entities*	*2*	*2*	*3*	*7*	**Share**
50	*Government and Seimas*	*Inadequate review process for current legislation*	*2*	*3*	*2*	*7*	**Share**
51	*Financial institutions*	*Inadequate verification of the Beneficial Owner*	*2*	*3*	*2*	*7*	**Avoid**
52	*Law Enforcement and Supervisory Authorities*	*Insufficient cooperation between FIU, Supervision Authorities and the reporting entities*	*2*	*2*	*3*	*7*	**Share**
53	*FIU, Supervisory Authorities*	*Failure to use appropriate tools, technologies, and methods for AML/CTF processes and*	*2*	*3*	*2*	*7*	**Mitigation**

No.	Owner	RISK ASSESSMENT					STAKEHOLDER RESPONSE
		Risk	Likelihood	Impact	Vulnerability	TOTAL	
		procedures					
54	*Financial institutions*	*Failure to use appropriate tools, technologies, and methods for AML/CTF processes and procedures*	*2*	*3*	*2*	*7*	**Mitigation**
55	*Financial institutions*	*Lack of internal databases on domestic PEPs and failure to check customer portfolio in these databases*	*2*	*3*	*2*	*7*	**Avoid**
56	*Law Enforcement Authorities*	*Mismanagement of confiscated goods*	*2*	*1*	*4*	*7*	**Share**
57	*Government and Seimas*	*Low level of political commitment to fighting crime*	*1*	*3*	*2*	*6*	**Share**
58	*Law Enforcement Authorities*	*Ineffective usage of information from cash declarations*	*2*	*2*	*2*	*6*	**Accept**
59	*Financial institutions*	*Inadequate verification of the transactions conducted by high risk customers or transactions with high risk countries*	*2*	*2*	*2*	*6*	**Accept**
60	*Financial institutions*	*Failure to verify the information provided by the customer*	*2*	*2*	*2*	*6*	**Accept**
61	*Financial institutions and DNFBPs*	*Committing money laundering and terrorism financing using domestic NPOs*	*1*	*3*	*2*	*6*	**Avoid**
62	*Financial institutions and DNFBPs*	*Committing money laundering and terrorism financing using private pension funds services*	*1*	*3*	*2*	*6*	**Avoid**
63	*Financial institutions and DNFBPs*	*Committing money laundering and terrorism financing using non-life insurance services*	*1*	*3*	*2*	*6*	**Avoid**
64	*Government and Supervisory Authorities*	*No system of registering or licensing service providers*	*1*	*4*	*1*	*6*	**Mitigation**
65	*Supervisory Authorities, Financial institutions and DNFBPs*	*Inefficiency of compliance audits*	*2*	*2*	*2*	*6*	**Accept**

No.	Owner	RISK ASSESSMENT					STAKEHOLDER RESPONSE
		Risk	Likelihood	Impact	Vulnerability	TOTAL	
66	*Financial institutions*	*Lack of awareness on ML/TF risks and inability to apply an effective risk based approach*	*2*	*3*	*1*	*6*	**Accept**
67	*FIU, Law Enforcement and Prosecutorial Authorities*	*Insufficient alignment of ML/TF investigation between law enforcement institutions*	*2*	*2*	*2*	*6*	**Accept**
68	*FIU*	*Lack of capabilities of financial intelligence unit (FIU) to process the reports that it receives*	*1*	*3*	*2*	*6*	**Accept**
69	*Financial institutions and DNFBPs*	*No measures or inadequate measures to freeze without delay terrorist funds and assets*	*1*	*3*	*1*	*5*	**Accept**
70	*Lithuanian Seimas and Government*	*Regulation of charitable donations does not cover overseas donations*	*1*	*3*	*1*	*5*	**Accept**
71	*Lithuanian Seimas and Government*	*Political instability*	*1*	*3*	*1*	*5*	**Accept**
72	*Law Enforcement Authorities*	*Areas of social, ethnic or political conflict*	*1*	*3*	*1*	*5*	**Accept**
73	*Law Enforcement Authorities, Lithuanian Government and Seimas*	*Inadequate budget or other resources for investigation and prosecution*	*1*	*2*	*1*	*4*	**Accept**
74	*Financial institutions*	*Opaque relations between grantees and NPOs*	*1*	*2*	*1*	*4*	**Accept**
75	*FIU*	*Lack of periodical reports on ML/TF trends and typologies*	*1*	*2*	*1*	*4*	**Accept**
76	*Financial institutions*	*Failure of record keeping*	*1*	*2*	*1*	*4*	**Accept**
77	*DNFBPs*	*Failure of record keeping*	*1*	*2*	*1*	*4*	**Accept**
78	*Law Enforcement and Prosecutorial Authorities*	*Insufficient international co-operation in investigations on ML/FT issues*	*1*	*2*	*1*	*4*	**Accept**
79	*Lithuanian Seimas and Government*	*Significant population shifts*	*1*	*2*	*1*	*4*	**Accept**

No.	Owner	RISK ASSESSMENT					STAKEHOLDER RESPONSE
		Risk	Likelihood	Impact	Vulnerability	TOTAL	
80	*Law Enforcement Authorities*	*High level of cultural immigrant, emigrant or religious ties with jurisdictions at high risk of experiencing terrorism, political instability*	*1*	*2*	*1*	*4*	**Accept**
81	*Lithuanian Seimas and Government*	*High level of ethnic diversity of the population*	*1*	*1*	*1*	*3*	**Accept**

Appendix 5 – Low Risk Watch List

No.	Owner	Risk	RISK ASSESSMENT				STAKEHOLDER RESPONSE
			Likelihood	Impact	Vulnerability	TOTAL	
1	*Law Enforcement Authorities, Lithuanian Government and Seimas*	*Inadequate budget or other resources for investigation and prosecution*	*1*	*2*	*1*	*4*	**Accept**
2	*Financial institutions*	*Opaque relations between grantees and NPOs disbursing funds or resources to grantees*	*1*	*2*	*1*	*4*	**Accept**
3	*FIU*	*Lack of periodical reports on ML/TF trends and typologies*	*1*	*2*	*1*	*4*	**Accept**
4	*Financial institutions*	*Failure of record keeping*	*1*	*2*	*1*	*4*	**Accept**
5	*DNFBPs*	*Failure of record keeping*	*1*	*2*	*1*	*4*	**Accept**
6	*FIU*	*Lack of engagement or reluctance to engage regionally or internationally on AML/CFT issues, including on requests for assistance*	*1*	*2*	*1*	*4*	**Accept**
7	*Lithuanian Seimas and Government*	*Significant population shifts*	*1*	*2*	*1*	*4*	**Accept**
8	*Law Enforcement Authorities*	*High level of cultural immigrant, emigrant or religious ties with jurisdictions at high risk of experiencing terrorism, political instability, or both*	*1*	*2*	*1*	*4*	**Accept**
9	*Lithuanian Seimas and Government*	*High level of ethnic diversity of the population*	*1*	*1*	*1*	*3*	**Accept**