LITHUANIAN NATIONAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING

Vilnius, 2020

Contents

1. Introduction

In agreement with the Prevention of Money Laundering and Terrorist Financing Law of the Republic of Lithuania (PMLTFL)[1], The National Risk Assessment of Money Laundering and Terrorist Financing (NRA) is performed every 4 years. The aim of the NRA is to measure a current risk level of money laundering (ML) and terrorist financing (TF) in Lithuania and to establish specific risk management controls (mitigation measures).

The NRA assesses the money laundering and terrorist financing risks affecting the internal Lithuanian market and cross border activities that are of priority concern in Lithuania.

Lithuania published its first national risk assessment in 2015[2]. The second NRA was established according to the Supranational Risk Assessment (SNRA)[3] methodology in 2019. The details of the NRA methodology used in preparing this report are presented in Annex 1. NRA methodology. The current NRA report updates the information, analyses the present ML/TF risk and proposes comprehensive action to address them.

The purpose of this NRA is to identify and evaluate the ML/TF threats and vulnerabilities in Lithuania. Once ML/TF risk is properly understood, Lithuania will be able to implement anti-money laundering and counter terrorist financing (AML/CTF) measures taking into account affected products and sectors.

According to the PMLTFL, money laundering is defined as per below:

- The change of asset's legal status or asset transmission, in the knowledge that this asset was brought up from criminal activities or directly participated in such activities, aiming to conceal or disguise illegal asset origin or intending to aid perpetrators to avoid legal consequences.
- The concealing or disguise of the real asset nature, origin, source, placement, possession, transmission, ownership or other asset legislations, in the awareness that the asset was delivered from criminal activities or participated in such activities;
- The acquisition, management, usage or transmission of the asset, in the knowledge that the asset was delivered from criminal activities or participated in such activities;
- The preparation to participate, collaboration or initiative in any of the activities listed above.

Terrorist financing is money/funds gathering using any possible methods, aiming to use, or in the knowledge that the gathering will be used in terrorist financing or in criminal activities related to terrorism. The funds could be gathered from both legal activities, such as charity organizations, as well as from illegal activities, such as drug trafficking, fraud, people trafficking and etc.

[1] Prevention of Money Laundering and Terrorist Financing Law of the Republic of Lithuania https://e-seimas.lrs.lt/portal/legalActEditions/lt/TAD/TAIS.41300

[2] Lithuanian NRA of ML and TF (2015) http://www.fntt.lt/en/money-laundering-prevention/lithuanian-national-risk-assessment-of-money-laundering-and-terrorist-financing/228

[3] Supranational risk assessment https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf

Criminal activities such as illegal arms sales, smuggling, activities of organized crime, including drug trafficking and prostitution rings, as well as embezzlement, insider trading, bribery and computer fraud schemes can generate large profits and create the incentive to 'legitimize' the ill-gotten gains through money laundering.

2. Executive summary

The second Lithuanian NRA was performed based on the Supranational Risk Assessment (SNRA) methodology provided in Annex 1 of this report, combining qualitative and quantitative information and professional expertise.

Data for NRA was collected from a variety of international and national (public and private) sources, including international studies and reports (e.g. EU SNRA, Financial Action Task Force (FATF) , Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Moneyval), Organisation for Economic Co-operation and Development (OECD)) statistics provided by sampled obliged institutions and Financial Investigation Unit (FIU) and non-publicly available data from the supervisory authorities and law enforcement authorities. This was complemented with AML/CTF experts' opinion and regular high-level interactions with the concerned authorities as well as the private sector to enrich findings.

NRA was conducted assessing both threats and vulnerabilities in order to determine inherent ML/TF risk per sector and sub-sector and / or product on a scale of one to four (very low to very high). Under threats and vulnerabilities, ML and TF were assessed separately given the differing nature of offenses.

NRA identified 88 risk scenarios applicable to 19 sectors covered within the report based on which each sector and its product was assessed against ML and TF risk.

NRA results are summarized in the table below from the highest to the lowest exposure to ML risk:

No	Sector / Sub-sector / Product	Total risk score	Threat	Vulnerability
1.	Virtual currencies	4	4	4
2.	Advocates	4	4	4
3.	Trade in goods in cash	4	4	4
4.	Trade in real estate	4	4	4
5.	Trade in precious stones, precious metals	3.4	4	3
6.	Banking / Transfer of funds	3.4	4	3
7.	Banking / Cash deposits to current account	3.4	4	3
8.	Consumer credits and Leasing	3.4	4	3
9.	Accountants, auditors and tax advisors	3.4	4	3
10.	Notaries	3.4	4	3
11.	Gambling sector / Casinos (A category)	3.4	4	3
12.	Trade in movable cultural goods, antiques	3	3	3
13.	Banking / Related to all products	3	3	3
14.	Currency exchange offices	3	3	3
15.	Investment companies	3	3	3
16.	Money remmitance	3	3	3
17.	Payment / E-money institutions	3	3	3
18.	Gambling sector / Gaming machines (B category)	3	3	3

19.	Gambling sector / Betting	3	3	3
20.	Banking / Trade finance	2.8	4	2
21.	Banking / Currency exchange	2.8	4	2
22.	Credit unions	2.6	2	3
23.	Non-profit organizations / Religious organizations	2.6	2	3
24.	Non-profit organizations / Charities	2.6	2	3
25.	Gambling sector / Online gambling	2.4	3	2
26.	Banking / Credit	2	2	2
27.	Crowdfunding platforms	2	2	2
28.	Life insurance	2	2	2
29.	Gambling sector / Lotteries	2	2	2
30.	Bailiffs	1.8	3	1

NRA results are summarized in the table below from the highest to the lowest exposure to TF risk:

No	Sector / Sub-sector / Product	Total risk score	Threat	Vulnerability
1.	Virtual currencies	4	4	4
2.	Trade in goods in cash	4	4	4
3.	Trade in real estate	4	4	4
4.	Consumer credits and Leasing	3.6	3	4
5.	Advocates	3.4	4	3
6.	Trade in precious stones, precious metals	3	3	3
7.	Trade in movable cultural goods, antiques	3	3	3
8.	Banking / Transfer of funds	3	3	3
9.	Banking / Cash deposits to current account	3	3	3
10.	Currency exchange offices	3	3	3
11.	Money remmitance	3	3	3
12.	Payment / E-money institutions	3	3	3
13.	Non-profit organizations / Religious organizations	2.6	2	3
14.	Non-profit organizations / Charities	2.6	2	3
15.	Accountants, auditors and tax advisors	2.4	3	2
16.	Banking / Trade finance	2	2	2
17.	Banking / Credit	2	2	2
18.	Banking / Currency exchange	2	2	2
19.	Banking / Related to all products	2	2	2
20.	Crowdfunding platforms	2	2	2
21.	Credit unions	1	1	1
22.	Life insurance	1	1	1

3. Economic, geographical, political, legal environment

3.1. Economic environment

Since renewed independence in 1991 and transition from a centrally planned to a market economy, Lithuania has substantially raised well-being of its citizens. Thanks to a market-friendly environment, the country grew faster than most OECD countries over the past ten years. The financial system is resilient, and fiscal position stabilized after a long period of deficits and rising debt. However, wage and income inequality are high, fueling emigration. The population is ageing fast and declining, particularly because of emigration..

In order to achieve a more significant economic growth among all of the sectors, Lithuania will require to raise productivity which still remains well below the OECD average, and has slowed down in recent years. This calls for further easing of regulations for the non-EU workers employment, financial constraints for productive firms, and reducing shadow economy. Moreover, continuing governance reforms would enhance the performance of state-owned enterprises.

Each year, the labor force shrinks by 1% due to the rapid ageing and high emigration, requiring a comprehensive approach to the economic consequences. The pension reform "New Social Model" strengthened the sustainability of the pension system, but did little to reduce old-age poverty. The need to upgrade skills, especially of older workers, calls for a broad-based life-long-learning system. Migration policy, including a focused outreach to emigrants and a less restrictive approach to immigration, could help slow down the labor force decline[4].

Since 2015, Lithuania jumped thirteen places (from 24th to 11th) in World Bank ease of doing business index, start-up category globally[5]. Gross domestic product (GDP) per capita in Lithuania is 81% of the European Union (EU) average of EUR 16,606.1 ($19,089.7[6]).

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 EUR 1,317[7] (or EUR 833 net).

The financial sector in Lithuania is bank-centric (79.2 % of the financial system assets) and is largely concentrated around three foreign-owned banks. The banking services are mainly traditional and include trade financing, loans and deposits. The number and the value of the payments is growing each year[8]. Banks have been reducing their non-resident customer base for de-risking purposes, thus the number of higher risk non-resident customers appears to be very low. Lithuania has the lowest number of foreign

[4] "OECD Economic Survey. Lithuania Overview June 2018". http://www.oecd.org/economy/lithuania-economic-snapshot/

[5] The Word Bank, Ease of doing business index https://data.worldbank.org/indicator/IC.BUS.EASE.XQ?most_recent_value_desc=true

[6] The World Bank, GDP per capita 2018 https://data.worldbank.org/indicator/NY.GDP.PCAP.CD?locations=EU-LT

[7] From 1 January 2019, the rates of the state social insurance contributions paid by the employer and the employee were changed. Gross earnings were indexed 1.289.

[8] Bank of Lithuania https://www.lb.lt/uploads/documents/files/2019%2004%2003%20LB%20AML%20BFK%20pristatymas%20LRS.pdf

nationals and corporate (non-resident) deposits in the Baltic region (Lithuania 2.5%, Latvia 20.3%, and Estonia 7.3%[9]). In recent years, the Bank of Lithuania has aimed to create an attractive regulatory environment to foreign finance institutions and financial services (Fintech) start-ups in the country. In 2014, a residence-by-investment program was established to attract foreign businesses, here according to the program, living permits for investors were provided.

There is still a high level of shadow economy in Lithuania, which is exacerbated by tax offences and the widespread use of cash. The withdrawal, deposit and remittance of cash (through either money or value transfer services or physical transportation) are commonly used in money laundering schemes. With respect to the results of different researches, the scope of shadow economy in Lithuania in 2017 constituted 15-24%[10] of GDP.

3.2. Geographical environment

Lithuania is the most populous country of the Baltic States (approx. 2.8 million), which are situated in the eastern shore of the Baltic Sea in Europe. Lithuania covers an area of about 65,286 km^2. Lithuania lays on the east shore of Baltic sea and borders with Latvia in the north, Belarus in the east and south, and Poland and the Kaliningrad region of the Russian Federation in 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 103.7 km. Lithuania also has a 290 km[11] 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

Lithuania is regarded as a politically stable country. The Lithuanian legal system is principally based on the legal traditions of Continental Europe and is grounded on the Constitution of the Republic of Lithuania and safeguarded by the Constitutional Court of the Republic of Lithuania.

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

[9]Bank of Lithuania, Estonian and Latvian Supervisory authorities
https://www.lb.lt/uploads/documents/files/2019%2004%2003%20LB%20AML%20BFK%20pristatymas%20LRS.pdf
[10] Medina L. and Schneider F., International Monetary Fund, 2018
https://www.imf.org/en/Publications/WP/Issues/2018/01/25/Shadow-Economies-Around-the-World-What-Did-We-Learn-Over-the-Last-20-Years-45583
[11] National Land Service Under The Ministry of Agriculture of The Republic of Lithuania
http://www.nzt.lt/go.php/lit/Valstybes-sienos-demarkavimas

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 which 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 22 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 (12)[12] are the courts of general jurisdiction which are dealing with civil and criminal cases. District courts also hear cases of administrative offences coming within their jurisdiction by law.

The Supreme Administrative Court of Lithuania (1) and regional administrative courts (2) are courts of special jurisdiction hearing disputes arising from administrative legal relations.

The Constitutional Court of the Republic of Lithuania[13] 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.

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 government institutions, courts, all enterprises, institutions and organizations, officials and citizens (erga omnes).

The Prosecution Service of the Republic of Lithuania is a public institution which performs the functions described in the legal acts of the Republic of Lithuania, and is responsible for the arrangement and execution of pre-trial investigations, the public prosecution in criminal cases, the protection of a public interest, thus ensuring the legitimacy and assisting 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.

[12] Lithuanian Courts https://www.teismai.lt/en/courts/judicial-system/650

[13] The Constitutional Court of The Republic of Lithuania https://www.lrkt.lt/en/about-the-court/activity/competence/182

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 of the Republic of Lithuania, Military Police, the Financial Crime Investigation Service, the Customs Authorities of the Republic of Lithuania, the State 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 their activities.

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

Each 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 disclose the criminal activities in a timely manner.

In the Lithuanian legal system, the principal body of law is the statute. 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. Organized crime[14]

Regular monitoring and analysis of organized crime by Lithuanian Criminal Police Bureau revealed that in 2018 most of the organized crime groups (OCG) have been involved in illicit drug trafficking and smuggling, theft of transport vehicles, smuggling of excise goods, illicit possession of firearms, extortion, theft abroad and robbery (which generates the largest illegal proceeds). As in previous years, the proceeds of crime are mainly used to improve the welfare of perpetrators. Also, members of OCG invest in legal business: real estate trading, various brokerage services, and trucking companies to legalize proceeds of crime.

The Lithuanian organized crime groups operate on a territorial basis, with the most dangerous groups being geographically concentrated in major cities.

Organized crime is also expanding its operations abroad. In recent years, Spain, the Netherlands and the Scandinavian countries have been linked to illicit drug trafficking. The most popular countries in which thefts continue are Germany and Scandinavia. Specifically car theft is dominating in Germany. This is influenced by the geographical location of the countries, which facilitates the transportation of stolen items to Lithuania. The most popular foreign countries where the Lithuanian organized crime groups operate are Spain, Scandinavian countries, Germany, Netherlands and Russia.

[14] Lithuanian Criminal Police bureau information

The ongoing monitoring and control of OCG has shown that the organized crime pays great attention to the self-protection measures in both of the planning and the execution of the crime. Organized crime groups are flexible and often engage in poly-crime, with potential cooperation between groups for the highest financial gain.

Additional information characterizing Organized crime groups (OCGs)

- Major challenges faced with OCGs:
    - OCG member mobility (both nationally and internationally);
    - OCG active international outreach;
    - OCG confidential communication possibilities;
    - OCG's performed conspiracy (members are being very cautious, they use all available knowledge of methods how to conduct investigative actions, take physical protection measures - alarms, installing video surveillance systems, using services of only trusted individuals or public services – renting cars, not owning any valuable assets, using their own established companies or legally operating entities, which can be influenced by OCG; some individuals are employed to display official income);
    - When one OCG cannot and another one can, the capabilities, experience, services or expertise of another OCG are used.

- The main illegal activity and the type of crime committed:
    - For several years in a row, the activities conducted by OCGs have remained unchanged with crimes committed both in Lithuania and abroad mostly involving illicit drug trafficking. In addition, there have also been vehicle thefts abroad, unlawful disposal and smuggling of excise goods, unauthorized possession of firearms, extortion, theft and robbery abroad.
- On modus operandi (MO), intimidation, bribery:
    - MO - illegal activities to maximize material / property related benefits. Legalization of financial assets resulting from crime activities by investing in business (logistics, real estate, automobile repair shops, car rental, pawn-shops);
    - Distinguished isolated cases of resistance to police officers;
    - Intimidation - inside OCG only to maintain order;
    - Bribery - unobservable or rare cases ("information shopping").

- Over the last three years, 419 persons, involved in crimes committed as organized groups or members of a criminal organization, have been registered in Lithuania (in 2017 - 185, in 2018 - 133, in 2019 – 101).
- According to the information available, the main purpose of OCG activities is aiming to material and asset gain. To achieve these goals, members of the OCG seek to be unsighted, not to give themselves away and remain non-public; violence directed to the outside of the OCG is not used. As a result, in most cases, Lithuanian Criminal Police Bureau does not track victims or witnesses when investigating crimes of OCG. In order to uncover OCG, proactive criminal intelligence is used and, through collected and documented information / material, crimes committed by OCG are uncovered and OCG decomposed. The individuals of the most dangerous groups, the priorities of the investigations, are more than often prosecuted and convicted.

4.2. Terrorist financing[15]

The Government of the Republic of Lithuania has ruled a low level of terrorist threat in Lithuania (ruling No. 93, 2015).

No organized groups motivated by extremist ideologies with the intent and capacity to commit terrorist acts have been identified in Lithuania in the last four years. No information has been received regarding the direct threat posed by international terrorist organizations to Lithuania, as well as publicly disseminated threats of terrorist acts or calls for their execution against Lithuania. No data is available on persons leaving Lithuania for conflict regions or on recruitment to participate in terrorist activities abroad.

Lithuania faces an indirect risk from international terrorism, which has remained as a serious threat in Europe in 2019. The main sources of threat are the terrorist organizations: the Islamic State of Iraq and Syria, Al Qaeda and the Islamist groups that support them, and individual radicals in EU countries. Terrorism tendencies in the EU countries do not have a direct impact on the situation in Lithuania, however the security situations of the EU member states are interrelated. Supporters of Islamist extremism make use of the opportunity to move freely within the Schengen area, at the same time increasing risks – in Lithuania as well – such as radicalization, extremism propaganda, organizing logistics and financing, recruiting and forming extremist clusters or organizing illegal migration. Extremists can use Lithuania for transit, hiding, and planning attacks against other countries.

Over the last few years, groups and individuals promoting right-wing extremism ideologies have become notably more active around the world. Proponents of these views commit an increasing number of casualty-demanding terrorist acts and ideologically motivated murders. A significant part of the attempts to commit this type of crimes is intercepted by intelligence or law enforcement agencies and do not have greater resonance in society. In 2018-2019, the number of individuals sympathizing with one of the most radical forms of neo-Nazism - Siege ideology - is growing in Europe, as a result, such tendency increases the likelihood of terrorist acts and other violent crimes.

The State Security Department of Lithuania (later – SSD) estimates that, taking into account the above information on the terrorist situation, the level of terrorist financing risk in Lithuania is assessed as low. Since 2015, when the State Security Department of Lithuania submitted information for national risk assessment, no cases of financing of foreign terrorist organizations and sponsors in Lithuania have been identified. However, the risk of terrorist financing may arise even in the countries where the terrorist threat level is low, as funds generated by performing lawful activities or crime may be used to support terrorists. Terrorist financing schemes can be difficult to track down, for example through social networks, crowdfunding, charity or NGO cover, cryptocurrencies, electronic payment instruments, complex chains of transfers of funds.

In the last few years, there has been a growing trend in Western countries when individual extremists without direct contacts with a terrorist organization and no support from it, independently raise funds for an uncomplicated and inexpensive attack or use easily accessible tools (knives, cars). On numerous

[15] The State Security Department of Lithuania information

occasions, extremists used their salaries or benefit allowances for terrorist crimes, sold their assets, received bank loans, traded counterfeit goods, and were engaged in financial fraud, robbery or theft.

It is not excluded that third country nationals permanently or temporarily residing in Lithuania, especially those from countries with a high risk of extremism, and extremism supporters can promote terrorist organizations operating abroad and persons associated with them through various formal or informal means of transfer of funds, cash couriers and mediators, including Hawala and other informal value transfer systems.

5. Overview of STRs

The number of suspicious transaction reports (STR) and cash transaction reports (CTR) has increased significantly since the first NRA. These reports, created by various financial institutions, obliged entities and foreign financial intelligence units, have been sent to Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania (FCIS). The total number of reports has increased by 177%.

A big part of STRs is received from banking sector. From 2016 to 2019 there has been a decrease in STRs sent from Designated Non-Financial Business or Profession (DNFBP) sector, however, there has been a rise in reports from payment/e-money institutions and money remittance offices.

Although during the last four years number of reports concerning Lithuanian natural and legal persons has risen, there has been a significant increase in STRs regarding foreign natural and legal persons in 2019.

No.	Sector	Number of STRs			
		2016	2017	2018	2019
1.	Banks and branches of foreign banks	302	509	854	780
2.	Financial institutions except banks	26	78	122	272
3.	Money remittance	84	121	222	353
4.	Designated Non-Financial Business or Profession (DNFBP)	108	94	78	38
5.	Foreign Financial Intelligence Units	21	33	92	58
	Total	541	835	1368	1501

Trends revealed after the analysis of the received STRs:

- **Social engineering fraud**. At the beginning, STRs regarding social engineering fraud noting psychological manipulations (mostly phone calls or other electronic means of communication) were received. Later intrusions into e-mail communications of the companies were reported. The perpetrators pretended to be partners and were asking to direct payments to the accounts

opened in other credit institutions. Examples of such fraud include emails adjusted by perpetrators or containing viruses, where information on fictitious contract is stated: contract, VAT invoice, acts of work, the name and the bank account number of the recipient. The accountant is manipulated to make the required transfer to a company which has not provided any services. In these cases the accounts used can be the ones opened by perpetrators, where no specific transactions connected to their businesses or their employees take place. Such companies often do not have any employees and their managers, who open the accounts, are young persons or foreigners. After such transactions occur, the companies aim to withdraw the cash or transfer the money to a foreign country.

The number of social engineering fraud cases has also increased, when individual persons, citizens of EU member States, came to Lithuania solely to open their accounts. Then the money which was obtained by criminal means was either immediately transferred abroad or withdrawn in cash in foreign countries. Fortunately, Lithuanian credit institutions received bank SWIFT messages each time such cases appeared. It has been discovered, that the amounts, which used to reach hundred thousand euros have decreased to thousands or ten thousand euros, however there has been an increase in the number of such transactions.

- **Fraud using cryptocurrency.** There has been an increase in the number of cases when perpetrators manipulated Lithuanian and foreign natural persons and made virtual currency investment offers. The schemers created investment advertisements on internet websites, attracting people to 'profitable' investments. When natural persons contacted financial institutions providing such services, they were offered to open accounts and transfer from hundreds to a few thousand euros, which presumably were invested into cryptocurrencies. In reality, the investment did not take place and the perpetrators took over the money in the account. Persons, who comprehended their losses, reported such events to financial institutions and requested refunds compensating the fraud activities.

- **Shell companies and suspicious cash operations**. For many years, this type of fraud has maintained their high tendency. During the financial operations analysis, suspicious Lithuanian companies were detected. Such companies' representatives withdrew significant amounts of money from their bank accounts. These companies often were newly created or their managers and shareholders had just changed. In all of the cases, there were one of few employees and the firm did not provide filled declarations, did not pay taxes and did not have a physical location. Money which was transferred to the company's bank account was immediately transferred to other firms in the criminal chain or withdrawn from automated teller machines (ATMs) in Lithuania. Such firms include international transfer of cargo, construction work, consultations, vehicles repair and other.

- **Money transit transactions.** Some offshore companies and natural persons use foreign financial institution accounts as transit passages to complicate the identification of their recipient and the real transaction purpose. The money is transferred for no apparent reason or economic background to foreign bank accounts, from which the payment is made to the real beneficiary.

The payment institutions often have difficulties communicating with the persons who opened the accounts initially, since there exist language, cultural and ethnic barriers.

- **"Money mules".** "Money mules" typology is when the persons involved in criminal offence find and recruit the persons for financial operations. The FCIS receive reports on the individual persons of the Republic of Lithuania and the foreign citizens related to the Republic of Lithuania receiving or transferring suspicious money through money transfer systems. Then, an investigation procedure is carried out and it is revealed whether the persons relate to OCG, distribution of drugs, human trafficking or prostitution on the international level. The information is transferred to the Lithuanian Criminal Police Bureau and FCIS for further investigation.

Cash transaction reports (CTRs)

According to the PMLTFL, FCIS is informed about cash transactions, when the transaction amount is, or exceeds 15 000 EUR, or is an equivalent amount in a foreign currency. Looking at 2016-2019, the number of such reports has increased by 89 %. CTRs in banking sector have risen even more.

No.	Sector	Number of CTRs			
		2016	2017	2018	2019
1.	Banks and branches of foreign banks	548 139	562 620	669 626	1 050 821
2.	Financial sector, except forbanks	2 027	2 714	3 086	3 068
3.	Notaries	10 623	9 383	8 267	6 970
4.	Other entities	2 453	1 593	546	674
5.	Customs reports on cash declarations	1 098	3 074	2 197	3 979
	Total	564 340	579 384	683 722	1 065 512

6. Stakeholders

The Lithuanian AML/CTF system consists of four interconnected components:

1. The FIU, which is the main institution coordinating the implementation of money laundering prevention measures in the Republic of Lithuania;
2. The law enforcement and other state authorities;
3. The supervision and regulation authorities; and
4. The financial institutions and other entities.

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

Authorities[16] defined in the table below (no. 1 to 8) must appoint senior staff to organize the implementation measures to prevent ML/TF and to liaise with the Financial Crime Investigation Service.

No	Regulatory and Supervisory authorities	Number of employees assigned to AML/CTF (2019)
1.	The Bank of Lithuania	9
2.	The Department of Cultural Heritage Under the Ministry of Culture	2
3.	The Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania	5
4.	The Lithuanian Bar Association	6
5.	The Chamber of Notaries	4
6.	The Lithuanian Chamber of Auditors	3
7.	The Chamber of Judicial Officers of Lithuania (Bailiffs)	14
8.	Lithuanian Assay Office	1
9.	Financial Crime Investigation Service under The Ministry of the Interior of the Republic of Lithuania	19
10.	Customs of the Republic of Lithuania	1

6.1. Financial Intelligence Unit (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 a law enforcement body, which mission is to protect the state financial system by disclosing criminal actions and other violations of law. FCIS implements AML/CTF measures in order to establish an effective national AML system and ensure its proper functioning, as well as conducts pre-trial investigation of legalization of the property derived from criminal activity.

Also, the FCIS is the main national institution which coordinates the cooperation of all institutions performing AML measures in Lithuania. FCIS is qualified to access classified financial information provided by both Lithuanian and foreign countries institutions working on AML/CTF measures, as well as financial institutions and other obliged entities that seeking to establish the criteria for identifying possible money laundering and suspicious monetary operations or transactions. Also FCIS supervises, regularly reviews and collects information on international financial sanctions from the financial institutions and other obliged entities.

The main unit of the FCIS implementing AML/CTF measures and analysis of STRs is Money Laundering Prevention Board (hereinafter – MLPB). MLPB is obliged to[17]:

1. Collect and register the information about the monetary operations and transactions of the customer and about the customer carrying out such operations and transactions;

[16] Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania
[17] Financial Crime Investigation Service http://www.fntt.lt/en/money-laundering-prevention/activities/226

2. Accumulate, analyse and publish the information relating to the implementation of money laundering and terrorist financing prevention measures;
3. Provide the information about the monetary operations and transactions carried out by the customer to the law enforcement and other state institutions;
4. Provide criteria for identifying possible money laundering and terrorist financing and suspicious or unusual monetary operations or transactions to financial institutions and other entities;
5. Inform financial institutions and other obliged entities, law enforcement and other state institutions on the results of the analyses related to their STRs as well as on the observed criteria of possible money laundering and terrorist financing or other violations; and
6. Evaluate the legal acts and submit proposals on the improvements following the international standards and recommendations.

As a Financial Intelligence Unit, the FCIS ensures a competent cooperation with the national institutions, as well as with foreign FIUs and international organizations seeking to identify and supervise the criminal activities related to ML and TF, and also identify system's threats, vulnerabilities and apply the most appropriate strategies.

In addition, the FCIS offers support on AML/CTF issues to the public and private sectors that fall under the AML/CTF regulations.

Under the international regulations, this authority must receive and analyze the STRs. Based on the performed analyses, FCIS releases the reports on AML/CTF activities annually.

6.2. Law Enforcement and other state authorities

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

- Prosecutor General'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; and
- The State Security Department.

Prosecutor General's Office is a state institution performing the functions established by the Constitution of the Republic of Lithuania, the Law on Prosecution Service or other laws. The Prosecution Service functions:

- Organises and directs pre-trial investigation;
- Co-ordinates the actions of the pre-trial investigation bodies;
- Controls the activities of pre-trial investigation officers in criminal proceedings;
- Prosecutes on behalf of the State;

- Supervises the submission of the judgements for enforcement and the enforcement thereof;
- Conducts pre-trial investigation or individual actions of pre-trial investigation;
- Protects the public interest;
- Examines petitions, applications and complaints submitted by individuals;
- Takes part in the drawing up and implementation of national and international crime prevention programs;
- Takes part in the legislative process.
- Perform other functions established by law.

The Customs Department under the Ministry of Finance of the Republic of Lithuania (Customs Department) is a state institution, which supervises international trade. Customs Department which is one of Europe Union countries members customs administration, contributes to the promotion of fair and open trade, European Union internal market performance, mutual market policy and other, trade related European Union policy measures conduction as well as the safeguarding of the supply chain of the goods. Customs is responsible for controlling the cash entering or leaving Lithuania.

The State Tax Inspectorate (STI) is responsible for the administration of taxes, with the exception of customs duties. The STI cooperates with the Financial Crime Investigation Service (FCIS) under the Ministry of Interior (MoI) to detect, prevent and suppress ML/TF. The STI and the FCIS exchange information and provide data, such as supervision of the activities of non-profit organizations (NPOs) and suspicious activities reports to the FCIS, where suspicious information has been uncovered in the course of daily duties of tax officials.

The State Security Department of the Republic of Lithuania (SSD) is the institution accountable to the President of the State and Lithuanian Parliament Seimas and its mission is to protect from the threats to the state, its sovereignty, and Constitutional Order. In accordance with the Lithuanian National Law of Security Principles , the State Security Department must annually prepare the Assessment of the Threats to the National Security.

The SSD coordinates fight against terrorism in institutions of the Republic of Lithuania in accordance to the Lithuanian National Law of Security Principles. The SSD is also one of the 12 responsible institutions for the prevention of TF and ML, pursuant to the Prevention of Money Laundering and Terrorist Financing Law of the Republic of Lithuania, for providing criteria for other institutions on how to notice potential terrorist financing activities.

6.3. Regulatory and supervisory authorities

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 Judicial Officers of Lithuania (Bailiffs);
- The Lithuanian Assay Office; and
- The Department of Cultural Heritage Protection under the Ministry of Culture.

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, performed transactions or the business itself.

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 of the manager or suspension of the business license.

The Bank of Lithuania (BoI) is included among the most important state institutions. Its principal objective is to maintain the 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. Functions of the Bank of Lithuania[18]:

- Monetary policy. Together with the European Central Bank and other euro area central banks, BoL works towards achieving the primary objective of the single monetary policy – maintaining price stability in the euro area.
- Financial stability. BoL aims to contribute to the stability of Lithuania's financial system; hence, it constantly monitors and assesses vulnerabilities in the system as well as takes measures to ward them off. In pursuing this goal, BoI not only carries out a full-fledged analysis of the financial system, but also actively mitigates threats to it, thereby implementing macroprudential policy.
- Payments. In terms of the country's economic and financial system, BoL ensures stable and efficient operation of payment and securities settlement systems by providing settlement services to banks and other payment service providers, as well as overseeing payment and securities settlement systems. BoL also encourage retail payments, used by residents and enterprises, and their competitiveness and progress in the market.
- Economic analysis and projections. Four times a year, having assessed economic development prospects, BoL publishes the latest projections for GDP, inflation, wages, unemployment rate, and other key economic indicators.
- Research. Being a center of the competency in economic and financial markets, BoL develops research among its units. The results of the researches aid to achieve monetary and economic policy resolutions, as well as expand the science of economics.
- Cash. The Bank of Lithuania supplies Lithuania with euro cash. It issues into and withdraws from circulation euro banknotes and coins.
- Management of Lithuania's financial assets. Financial assets under management comprise over EUR 5 billion and 5.8 tons of gold. The purpose of financial assets is to ensure the stability of the financial system in Lithuania and the euro area, create conditions for smooth monetary policy implementation, ensure the financial independence of the Bank of Lithuania and provide a buffer

[18] Bank of Lithuania https://www.lb.lt/lt/veiklos-sritys

for the country to withstand economic and financial shocks as well as other extraordinary circumstances.

- Supervision of financial market participants. BoL currently supervises over 470 financial market participants – banks, credit unions, insurance undertakings, payment institutions, electronic payment institutions, investment companies, consumer credit providers, issuers, etc. In supervising the financial market, BoL uses risk-based supervision, meaning that BoL allocates its resources towards systemically most significant financial market participants or financial services and products posing the highest risk for consumers. BoL supervises the financial market by following the financial market supervision policy.
- Economic and financial education. BoL, acting jointly with another four state institutions, aims to improve the economic and financial education of the country's residents.

The Gaming Control Authority is an institution under the Ministry of Finance of the Republic of Lithuania that, together with other state and municipal institutions, takes part in the implementation of the state policy in the area of gaming and conducts gaming control to ensure fair and transparent gaming activities and to protect the rights and legal interests of players.

Also, Gaming Control Authority is responsible for supervision and control of the organization of national lotteries. The institution supervises the lotteries to ensure fair and liquid activities and to protect the interests and the rights of the players and lottery operators.

Main functions of the Gaming Control Authority are:

- issue and cancel gaming and national lottery licenses;
- issue permits to open gaming machine halls, bingo halls, betting and totalizator stations and gaming establishments (casinos);
- control compliance of gaming and lottery operators with the requirements of the laws and other legal acts regulating the operation of gaming and lotteries;
- prepare legal acts regulating the operation of gaming;
- administer the Register of Gaming Devices of Lithuania; and
- administer the Register of Persons Restricted from Participation in Gambling.

The Gaming Control Authority is also responsible for other entities control, making sure that the gaming and national lottery organizers follow the laws and legal acts regarding gaming and lotteries organization in Lithuania.

Lithuanian Bar Association – self-regulatory institution of advocates, which brings together all lawyers, coordinates their activities, represents their interests in national institutions, international and foreign organisations, as well as performs additional functions. Since 2017, the Association is responsible for the prevention of money laundering and / or terrorist financing. PMLTFL obliges the Lithuanian Bar Association to approve AML/CTF instructions for lawyers and their assistants, to supervise the AML/CTF procedures and advise attorneys and lawyers on the implementation of the regulations of the Lithuanian Bar Association.

Chamber of Notaries – self-governing body, which assembles 247 notaries working in Lithuania. Major objectives and functions of the Chamber of Notaries:

- to exercise the self-governance of notaries;
- to coordinate the activities of notaries;
- to take care of the legal culture and professional development of notaries;
- to make the notarial practice more uniform;
- to draft regulatory legal acts related to the notaries and submit them to the Ministry of Justice of the Republic of Lithuania; and
- to inform the public about the functions carried out by notaries.

A public legal entity the **Lithuanian Chamber of Auditors** 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 Judicial Officers of Lithuania (Bailiffs) acts pursuant to the Republic of Lithuania Law on Judicial Officers, the Republic of Lithuania Law on Associations and the Articles of Association of the Chamber of Judicial Officers of Lithuania. The Chamber of Bailiffs brings together 95 firms, which employ 113 bailiffs. It also coordinates the activities of bailiffs, represents the interests of bailiffs, organizes and carries out the bailiffs and bailiffs' assistants qualification etc.

The Lithuanian Assay Office performs 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 checks the economic entities of the Republic of Lithuania and other institutions, regardless from their authorities and form of the property, that buy, sell, use, store, process the precious metals, gems, their scrap and waste, or produce the products made from them, as well as performs other functions assigned by law. The main goals of the activity of the Lithuanian Assay Office are:

- Ensure that all articles of precious metals and gems intended for sale in Republic of Lithuania will be examined and marked in compliance with the requirements of the Law on State Supervision of Precious Metals and Gems, state standards and other regulatory enactments;
- Evaluate and improve the control of economic entities, acting in the field of precious metals and gems, articles of precious metals and gems; and
- Achieve that all EU tasks in the field of precious metals and gems would be implemented without violation of interests of Lithuanian manufacturers, suppliers, users and state.

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 determining damage and evaluating losses of the movable cultural goods registered in the Cultural goods register, maintaining accounting and control of cultural heritage, as well as presenting the 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. 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.

6.4. Financial Institutions

The following financial institutions have been identified as stakeholders of the NRA in 2019:

FINANCIAL SECTOR Entity type	Number of financial entities in 2019
Banks	7
Branches of foreign banks	8
Credit Unions	63
Life insurance	8
Payment institutions	49
E-money institutions	55
Currency exchange offices	24
Consumer credit providers	56
Crowdfunding platform operators	11

6.5. Designated Non-Financial Businesses and Professions (DNFBP)

The table below displays the numbers of entities performing non-financial commercial activities in Lithuania in 2019, which are obliged to AML/CTF regulations.

NON-FINANCIAL SECTOR Entity	Number of non-financial entities in 2019
Casinos (A category; land-based)[19]	3
Gaming machines (B category)	7
Betting	5
Online gambling	6
Lotteries	6
Dealers in precious metals and stones[20]	1,949
Persons licensed to deal in antiques[21]	87
Lawyers (Advocates) [22]	2,213
Notaries[23]	247
Audit firms[24]	177
Bailiffs[25]	114

[19] The Gaming Control Authority https://lpt.lrv.lt/lt/losimu-organizatoriai/veiklos-ataskaitos
[20] The Lithuanian Assay Office https://lpr.lrv.lt/lt/ukio-subjektu-sarasas
[21] Department of Cultural Heritage under The Ministry of Culture http://www.kpd.lt/licenzijos-prekiauti-antikvariniais-daiktais/
[22] Lithuanian Bar Association http://www.advokatura.lt/lt/apie-advokatura/veiklos-ataskaitos.html
[23] Chamber of Notaries https://www.notarurumai.lt/notaru-rumai/veikla
[24] The Lithuanian Chamber of Auditors https://lar.lt/www/new/news.php
[25] The Chamber of Judicial Officers of Lithuania (Bailiffs) https://www.antstoliurumai.lt/

Accounting and tax consultation companies as well as such individuals providing such services[26]	2170

[26] Department of Statistics of Lithuania https://osp.stat.gov.lt/ and The Authority of Audit, Accounting, Property Valuation and Insolvency management http://www.avnt.lt/

7. AML / CTF Risk Assessment

7.1. Financial sector

7.1.1. Banking

7.1.1.1. Product: Transfer of funds

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrator deposits large amounts of cash to his bank account and makes smaller transfers to other account(s) in a timely manner, so escaping transaction limits. 2. The business, which does not have any legitimate activity, and therefore no legitimate source of funds, perform fictitious transactions in order to disguise criminal proceeds as legitimate earnings from trade in goods and services, especially intangible services such as marketing, IT services and consulting. 3. Companies set up fictitious loans with each other to justify transfers of funds of illegal origin. 4. Perpetrator launders money by making the instant payment to/from dormant account. 5. The Commonwealth of Independent States (CIS) countries' companies participating in projects financed by their governments hire Lithuanian private companies as subcontractors with higher fees than market average allowing funds of politically exposed persons (PEPs) of CIS countries to reach Lithuanian banks accounts.

Threat || *Money laundering*	**Level: 3-4**
Modus operandi is easy to access and does not require specific expertise or techniques to launder proceeds of crime. Perpetrators themselves or through close associates integrate illicit funds using transfer of funds into the financial system by making complex schemes, fictitious goods and services or using other banking system weaknesses and loopholes.	

Threat || *Terrorist financing*	**Level: 3**
Transfer of funds to high-risk regions is convenient way to finance terrorist activities. Banks accounts are easily accessible, especially when legitimate funds are used, and thus they do not trigger any suspicion when the bank account is opened. Terrorist groups do not experience specific challenges in hiding the real beneficiary of the funds or the exact purpose of the transaction (destination of funds) given that they may still include family members or relatives in the ownership chain. This requires basic planning and basic knowledge of how the banking systems work.	

Vulnerability || *Money laundering*	**Level: 2-3**
Domestic payments as well as the international ones are becoming more popular due to the globalization, favorable regulatory environment, innovations and new technologies. Therefore banks have to create specific customer due diligence and transaction monitoring systems, which would constantly review customer's bank operations and business relationship activities. Current transaction monitoring systems employed by banks tend to be based on established rules (for example transfer limits) but not on emerging possible risks and their scenarios depending on crime typologies. Many transaction alerts are generated, but it results only in a few STRs (chapter 5), i.e.	

transaction monitoring systems generate a lot of false positive alerts. Difficulties arise due to the regulations within The Single European Payments Area (SEPA) and SWIFT world-wide bank network: banks are not required to reconcile the recipient's name with account number, therefore perpetrators use other recipient's name in order to avoid the real name being matched in sanction lists. Banks also have difficulties to verify beneficial owners, especially of non-resident clients and to identify shell companies. Non-residents create 3.5% of all clients' portfolios. It is also noted that it is challenging to identify fictitious shell companies, since there exists a lack of competent institutions recommendations regarding these companies. The banks have a sufficient understanding of ML risks and implement adequate AML controls. In addition to that, the customers and beneficial owners' identification processes are regularly reviewed and updated. Transfers from Lithuania to countries outside the European Union represent a very small part, i.e. 0.4%[27] of the total number of transfers, which represents 3.6% of the total value of the transfer.

Vulnerability || *Terrorist financing*	**Level: 3**

In 2016-2018 banks provided a significantly small amount of reports regarding possible TF operations. Although the banking sector has a sufficient knowledge on TF risks, the banks have a limited access to applicable information. The systems and processes that the banks employ to combat the terrorist financing risk are the same as for money laundering prevention purposes, i.e. transaction monitoring rules are not specifically tailored for TF. According to the banks, the main tool which is used to control the TF risk is clients, beneficial owners, payment senders and recipients screening on the international sanctions lists. Financial sanctions target groups and individuals who are already acknowledged, whereas the TF risk often emanates from individuals who are not yet captured by the system. Therefore sanctions screening is an insufficient method for CTF. According to the State Security Department of Lithuania, there is a low level of terrorism threat in Lithuania. Possible TF mostly relates to foreign individuals, therefore the weaknesses in the control system mentioned above are lessened by the fact that almost 97 % of bank customers (both natural and legal persons) are residents, who in most of the cases (99%) were identified by face-to-face method.

Mitigation measures

1. Closely monitor dormant accounts. In particular, when an account identified as dormant becomes active as a result of initiation of a transaction, this event should trigger an alert and should be verified that this renewed activity on the account is not of suspicious nature.
2. Customer due diligence and transaction monitoring rules should be specifically tailored to combat TF, not only ML.
3. Conduct thematic inspections on how beneficial owner identification and verification requirements are implemented.
4. Provide specific guidelines to aid banks identify "shell companies".
5. Create the channel or platform for financial market participants (both private and public sectors) to share their knowledge on AML/CTF topics, for example, potential ML/TF schemes / typologies in area of transfer of funds.
6. Summarize STR data and share the knowledge on possible ML/TF schemes, which would enable market participants to see the "big picture" and adjust their ML / TF prevention processes.

[27] Bank of Lithuania, Estonian and Latvian Supervisory authorities
https://www.lb.lt/uploads/documents/files/2019%2004%2003%20LB%20AML%20BFK%20pristatymas%20LRS.pdf

7.1.1.2. Product: Trade finance

DESCRIPTION OF THE RISK SCENARIOS
1. Trade finance products such as letter of credit, guarantees and factoring may be used for money laundering and terrorist financing. Banks act as intermediaries to assist buyers and sellers by financing and covering the trade cycle funding gap, the amount of money needed to fund the ongoing operations or future development of a business. Most common techniques of trade finance money laundering involve moving illicit goods, falsifying documents, misrepresenting financial transactions and under- or over-invoicing the value of goods.

Threat || *Money laundering*	**Level: 3-4**
Perpetrators use trade finance products to justify the movement of criminal proceeds through banking channels, often using false documents for the trade of goods and services. It can potentially allow the rapid transfer of large sums by justifying an alleged economic purpose. While the required expertise and planning capacity is not negligible, the modus operandi is generally quite accessible, has a low cost and is relatively easy to exploit.	

Threat || *Terrorist financing*	**Level: 2**
Due to trade finance complexity, terrorists find trade finance not attractive channel to finance terrorist activities.	

Vulnerability || *Money laundering*	**Level: 2**
Although the banking sector has a sufficient knowledge of ML risks in trade finance, some parts of the sector are missing trade finance tailored transaction monitoring rules. However, turnover of all trade finance products in Lithuania compose up to 10% of the total turnover, making it a rather small proportion of the banks services portfolio.	

Vulnerability || *Terrorist financing*	**Level: 2**
94% of trade finance customers are residents, which makes this modus operandi less vulnerable in respect of terrorist financing. However, systems and processes that banks employ are not tailored specifically to TF prevention.	

Mitigation measures
1. Summarize STR data and share the knowledge on possible ML/TF schemes, which would enable market participants to see the full picture and adjust their ML/TF prevention processes. 2. Banks while performing enterprise wide risk assessment, have to assess impact of trade finance to ML / TF and tailor transaction monitoring system reducing ML/TF risk caused by this product.

7.1.1.3. Product: Credit

DESCRIPTION OF THE RISK SCENARIOS
1. Credit borrower repays outstanding loan payments with illicit funds. 2. Terrorists use credit cards to finance TF activities (acquire the necessary items for terrorism act).

Threat || *Money laundering*	Level: 2
Perpetrators use credit (including mortgages, credit cards) to finance the purchase of high value goods and then redeem the loans by cash. However, this product offers less money laundering potential than other financial products, since more knowledge on the product is required.	

Threat || *Terrorist financing*	Level: 2
Credit products provided by banks are less attractive to the terrorists as these products require a high level of knowledge and expertise, as well as the banks demand detailed documentation on the credit purpose and its owner.	

Vulnerability || *Money laundering*	Level: 2
Banking sector has proper transaction monitoring systems, however, verification of source of funds sometimes is rather formal and relies only on the answers provided by the customer and no additional verification documentation is required.	

Vulnerability || *Terrorist financing*	Level: 2
Although banks do not have specialized systems to control TF activities, they analyze the credit purposes and review its applications. According to the State Security Department data, terrorism threat level in Lithuania remains low and possible TF financing is mostly related to foreign individuals which create only 3% of all bank customers. 97% are residents, who in most of the cases (99%) were identified by face-to-face method.	

Mitigation measures
1. Ensure that all documents supporting / verifying client's source of funds are collected and maintained. 2. Ensure, that the transaction monitoring systems spot TF cases, when the credit cards are used.

7.1.1.4. Product: Cash currency exchange

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrators convert their illicit cash into another currency. 2. Perpetrators, in order to avoid their identification, split transactions and perform currency exchange in small amounts.

Threat || *Money laundering*	Level: 4
High volumes of cash currency can be easily converted, making it easy for perpetrators to exchange the illicit funds and deposit it to their accounts. Currency exchange does not require specific planning or expertise for money laundering purposes.	

Threat || *Terrorist financing*	Level: 2
Bringing currency into conflict zones is one of the main ways of financing the movement of foreign terrorist fighters. From a technical point of view, the conversion of funds does not require specific planning, knowledge or expertise and is quite easy to access. Terrorist groups may consider that currency exchange is as attractive as collecting or transferring funds to finance their activities.	

Vulnerability || *Money laundering*	Level: 2
The fact that currency exchange operations are cash based increases the sector's vulnerability. In the neighboring countries, there are higher limits when customer identification is required. In Lithuania, the limit amount is €3,000 (however, most banks identify a client despite the amount to be exchanged), while in Poland it is €15,000 and Estonia – €10,000. This fact makes Lithuania less attractive for perpetrators if they have a huge amount of illegal funds, which they want to exchange to other currency. Currency exchange service in banks is used by a small amount of non-resident customers. According to the data provided by the banks, in 2016-2018, less than 5% of non-resident clients changed currency equal to €3,000 or larger amounts. In addition, currency equal to €3,000 or larger amounts exchange consists on average less than 0.5% of banks turnover. Under legal regulations, client identification and cash transaction information must be provided to FIU if client's one-off cash transaction or number of related cash transactions equals or exceeds EUR 15,000 or equivalent amount in foreign currency. There exist issues in monitoring related transactions when clients are splitting exchange transactions up to EUR 3000 in order to avoid identification procedure. From December 2019, all largest banks in Lithuania ceased cash currency exchange service.	

Vulnerability || *Terrorist financing*	Level: 2
Although the banking sector has a strong KYC process and all of the capabilities to detect potentially suspicious transactions, the fact that the currency exchange operations are cash based increases the sector's vulnerability. Potential transactions linked to terrorist financing usually involve small amounts of cash that are more difficult to detect. Some banks do not use employed KYC and transactions monitoring systems, when providing cash currency exchange up to 3000 EUR and do not detect related transactions if a customer is not exceeding 3000 EUR per single transaction.	

Mitigation measures
1. Ensure that all banks have systems enabling to monitor related transactions and splitting transactions in area of cash currency exchange.

7.1.1.5. Product: Cash deposits to current account

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrators place cash from illegitimate or criminal sources into their current account. 2. Perpetrators use cash front businesses to inject cash revenues into financial system. 3. Terrorists, their supporters or facilitators place funds from legitimate or criminal sources into the financial system with a view to using it for terrorist purposes.

Threat || *Money laundering*	**Level: 4**
Modus operandi is one of the easiest ways to integrate illicit funds into the financial system. Deep planning and knowledge of banking systems is not necessary when depositing small amounts. However, the perpetrators require more in-depth understanding when working with larger amounts, thus they may use available expertise from the intermediaries.	

Threat || *Terrorist financing*	**Level: 3**
Using current accounts is easily accessible, especially when legitimate funds are used, thus they do not trigger any suspicion when the bank account is opened. Cash withdrawals (using ATMs in higher risk countries) allow cross-border movements, which makes this modus operandi rather attractive. This requires at least basic planning and basic knowledge of how the banking systems work.	

Vulnerability || *Money laundering*	**Level: 3**
Banks are shifting towards no cash operations and eventually will not accept cash operations at all, except for ATMs. During the period of 2016-2018, the value of cash transactions accounts for up to 7 % of the total turnover of bank customers. While the banking sector has an inherently high exposure to money laundering risk, it also has the best procedures and tools to detect it in comparison with the rest of the financial sector. There is a tendency of increasing cash deposits received from cryptocurrency cash-outs. However, currently there is a lack of technological tools to identify and verify legitimacy of such funds and recipients of cryptocurrency transactions.	

Vulnerability || *Terrorist financing*	**Level: 3**
Banks are exposed to terrorist financing risks as depositing cash to banking accounts represent the easiest way to introduce money into the financial system. The vulnerability is even higher when the origin of funds is legitimate. The risk awareness of the sector is good; however, monitoring rules employed by banks are not specifically tailored for terrorist financing prevention.	

Mitigation measures
1. Ensure that all documents supporting client's source of funds, especially related to funds from cryptocurrency trading, are collected, verified and maintained. 2. Ensure public (law enforcement authorities) – private sector cooperation to exchange information related to terrorist financing. 3. Perform thematic inspections focusing on assessing compliance of banks' AML / CTF measures against regulatory requirements.

4. Customer due diligence and transaction monitoring rules should be specifically tailored to combat TF, not only ML.

7.1.1.6. Related to all products

DESCRIPTION OF THE RISK SCENARIOS
1. Individuals establish fictitious low risk entities and later sell it to a perpetrator. 2. In situations when banks refuse to start business relationship with a non-resident individual, the non-resident individual sets up a company in Lithuania and opens a bank account as a legal person. Later such company acts as a "shell company" for money laundering purposes. 3. Perpetrators use genuine accounts of money mules to process illegal payments linked to terrorism, money laundering and other economic crimes.

Threat || *Money laundering*	**Level: 3**
The modus operandi is attractive for money launderers, even though it requires preparation and expenses. According to FCIS 2018 report, there are more cases where foreign individuals establish or start managing Lithuanian companies and open accounts in Lithuania. They make transit transfers or withdraw cash obtained from suspicious transactions in foreign ATMs. One of the risk scenarios defined by FCIS is when perpetrators find and employ individuals to perform monetary transfers.	

Threat || *Terrorist financing*	**Level: 2**
As modus operandi requires more planning and costs, it is less attractive to be used for terrorist financing.	

Vulnerability || *Money laundering*	**Level: 3**
Current transaction monitoring systems employed by banks tend to be based on established rules but not on emerging possible risks and their scenarios depending on crime typologies. Many transaction alerts are generated, but it results only in a few STRs, i.e. transaction monitoring systems generates a lot of false positive alerts. Banks also have difficulties to verify beneficial owners of non-residents (around 3.5% of all customers) using reliable and independent information. It is also difficult to identify shell companies and fictitious services due to the lack of guidance by authorities. In some banks KYC information for low risk clients is updated only once a year or even less often, which would allow a perpetrator, who bought a low risk legal entity, to use a bank account up to at least one year until KYC data is updated.	

Vulnerability || *Terrorist financing*	**Level: 2**
Although the banks have a sufficient knowledge of TF risk, they have a limited access to information related to TF risk. The banking sector maintains effective KYC system, however, processes that the banks employ to combat the terrorist financing risk are the same as for money laundering prevention purposes, i.e. transaction monitoring rules are not specifically tailored for TF, except sanctions screening. However, financial sanctions target individuals or groups that are already known to pose a threat, whereas the risk from terrorist financing often emanates from individuals who are not caught by the sanctions regime. According to the State Security Department, terrorism threat level remains	

low in Lithuania and the possible TF is mainly related to foreign individuals. This risk is lessened by the fact that around 97% of banks customers (both individual persons and legal entities) are residents who in most of the cases (99%) were identified by face-to-face method.

Mitigation measures
1. Provide specific guidelines to aid banks identify "shell companies". 2. Tailor customer due diligence and transaction monitoring process to combat TF, not only ML. 3. Ensure that KYC update process would allow timely identification of changes related to clients and its UBO data.

7.1.2. Credit unions

DESCRIPTION OF THE RISK SCENARIOS
1. Credit borrower repays outstanding credit payments with cash with illicit funds. 2. Credit union refinances loan for customer who uses fictitious agreement with third party loan lender. 3. Credit borrower uses the funds for different purpose than stated, for example to finance terrorists. 4. Perpetrators place cash from illegitimate or criminal sources into current account.

Threat || *Money laundering*	**Level: 2**
The modus operandi is attractive as it relates to cash operations and criminal organizations use it to finance the purchase of high value goods and then redeem the loans by using illicit funds.	

Threat || *Terrorist financing*	**Level: 1**
Although credit procedures in credit unions are more simple than in the banks and do not need specific knowledge and planning, modus operandi is not as popular among the terrorists since credit unions activities are rather focused on specific domestic region.	

Vulnerability || *Money laundering*	**Level: 3**
Credit unions are less aware of money laundering risk than the banking sector. The cash intensive nature of credit union services (on average one third of total turnover), makes it increasingly difficult to identify source of funds and increase the risk that the proceeds of crime are being used to repay loans or to accumulate into larger amounts in current account.	

Vulnerability || *Terrorist financing*	**Level: 1**
Credit unions are less informed about the TF risk than the banking sector. Some of the unions do not verify whether their credit is used for the stated purpose. However they do not have an international	

network and very small number of customers (less than 1%) are non-residents (according to the State Security Department, TF is mainly related to foreign individuals)

Mitigation measures
1. Ensure that all documents supporting / verifying client's source of funds are collected, assessed and maintained. 2. Ensure that the credits are used for the declared purpose. 3. Ensure that proper KYC and transaction monitoring procedures are implemented enabling reduction of ML/TF risk.

7.1.3. Crowdfunding platforms

DESCRIPTION OF THE RISK SCENARIOS
1. Criminal collects funds from legitimate sources using crowdfunding platform to fund terrorism. 2. With a help of crowdfunding platform, a perpetrator collects illicit funds from criminal activities using anonymous products like virtual currency. 3. Terrorists use "money mules" to collect money through the crowdfunding platform.

Threat || *Money laundering*	**Level: 2**
No evidence of using this modus operandi existing yet, but there is a possibility for perpetrators using the crowdfunding to launder money. The implementation of the risk scenario would require some expertise and can be costly.	

Threat || *Terrorist financing*	**Level: 2**
Terrorist groups may have the intent to use the crowdfunding techniques to collect funds, however this modus operandi requires more planning to hide the illicit intent in comparison with other products offered by the financial sector.	

Vulnerability || *Money laundering*	**Level: 2**
In Lithuania, crowdfunding activity is regulated and does not involve cash operations. All clients in this sector are residents. Crowdfunding platforms use electronic payment institutions as a third party for non-face-to-face client identification and do not have automated transaction-monitoring tools. The sector has also difficulties in verifying beneficial owners, PEPs and source of funds. The vulnerability of crowdfunding is higher if crowdfunding platforms allow use of virtual currencies or anonymous electronic money.	

Vulnerability || *Terrorist financing*	**Level: 2**
Vulnerability applicable for terrorist financing is the same as for money laundering.	

Mitigation measures
1. Increase regulatory supervision on crowdfunding entities in area of ML/TF prevention ensuring that the sector employs all ML/TF prevention measures required by legislation.

7.1.4. Currency exchange offices

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrators via third persons establish fictitious currency exchange office and infiltrate illicit funds from criminal activities. 2. Perpetrators convert their illicit cash into another currency. 3. Perpetrators split payments into smaller amounts thus avoiding identification.

Threat || *Money laundering*	Level: 3
Currency exchange does not require specific planning or expertise for money laundering, thus it is an attractive sector for the perpetrators to stock their illicit funds. High volumes of cash currency can be easily converted, making it easy to exchange the illegitimate capital.	

Threat || *Terrorist financing*	Level: 3
Bringing currency into conflict zones is one of the main ways of financing the movement of foreign terrorist fighters. From a technical point of view, the conversion of funds does not require specific planning, knowledge or expertise and is quite easy to access. Terrorist groups may consider that currency exchange is as attractive as collecting or transferring funds to finance their activities.	

Vulnerability || *Money laundering*	Level: 3
The knowledge of ML/TF risks is low among the currency exchange offices in Lithuania. The fact that currency exchange operations are cash based increases the sector's vulnerability. Lithuanian offices perform customer identification procedures when €3,000 or more is being exchanged. The limit is higher in the neighboring countries: €15,000 in Poland and €10,000 in Estonia. This makes Lithuania less attractive for perpetrators who own huge amounts of illegal funds, which they want to exchange to another currency. The vulnerability of this sector is increased by the fact that some offices do not use databases, but rather check the information manually, once it comes to international financial sanctions screening and investigating adverse media, identifying PEPs, restricted persons and other suspicious information. It is also difficult to track clients who are splitting the amounts up to €3,000 in order to avoid the identification process as the sector has not employed required systems. According to the national law, information on the head of the currency exchange office, shareholders and beneficial owners is submitted and assessed by the supervisory institution.	

Vulnerability || *Terrorist financing*	Level: 3
The fact that currency exchange operations potentially linked to terrorist financing usually involve small amounts of cash and the fact that currency exchange offices do not have measures to identify related transactions increases the sector's vulnerability.	

Mitigation measures
1. All currency exchange offices must employ systems, allowing monitoring of related transactions and splitting transactions performed by its customers. 2. Currency exchange offices should establish internal policies and procedures related to PEPs identification, verification and sanctions screening.

7.1.5. Investment companies

DESCRIPTION OF THE RISK SCENARIOS
1. Customers conducting securities trades on behalf of organized criminals, use illegitimate money to purchase securities and then integrate funds into financial institutions after selling those securities.

Threat || *Money laundering*	Level: 3
The increasing role of facilitators in money laundering schemes can make the sector more exposed to such threats; however, this modus operandi requires deep knowledge and technical expertise. Since the role of facilitators is essential to create opaque structures and hide the proceeds of criminal activities, the perpetrators do not favor this kind of risk scenario.	

Threat || *Terrorist financing*	Level: N/A
Not relevant.	

Vulnerability || *Money laundering*	Level: 3
Investment companies rely on other institutions' AML/CTF procedures since most of transactions come from bank accounts and little from e-money or payment institutions. Investment companies do not perform cash operations, however the sector is exposed to higher risk customers (high and higher risk customers make up to 98% of all clients), including politically exposed persons. Not all investment companies verify the source funds of its customers. Turnover of over the over-the-counter trades generates up to 45% of the total turnover.	

Vulnerability || *Terrorist financing*	Level: N/A
Not relevant.	

Mitigation measures
1. Ensure that investment companies apply all AML/CTF measures themselves instead of reliance on other financial sector participants. 2. Ensure a proper client review, including the identification of the customer and beneficial owner. 3. The supervisory authorities should assess the companies AML/CTF procedures, ensuring that the applied methodologies meet the legal acts requirements.

7.1.6. Consumer credits and Leasing

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrator, instead of the borrower, repays the credit using illicit funds. 2. Loan borrower uses the funds for different purpose than stated, for example to finance terrorists. 3. Perpetrator accelerates an agreed repayment schedule, either by means of lump sum repayments, or by means of early termination using funds emanated from a criminal lifestyle.

Threat || *Money laundering*	**Level: 4**
The modus operandi offer less money laundering potential than other financial products, but criminal organizations use it to finance the purchase of high value goods and then redeem the loans by using illicit funds.	

Threat || *Terrorist financing*	**Level: 3**
The low value loans are attractive for the terrorists since they do not require a high level of expertise or planning.	

Vulnerability || *Money laundering*	**Level: 3**
Consumer credit and leasing institutions in Lithuania do not operate in cash. The customers of consumer credit entities are solely individual persons and 99% are residents. This makes the sector less risky in terms of ML. However, because of the small amounts borrowed, the sector is less aware of the money laundering risks. Not all consumer credit institutions have databases to investigate customer's PEP status, exposure to sanctions and adverse media. The sector also does not have transaction monitoring systems. Moreover, consumer credit entities do not check the payee of credit repayments because their focus is to receive the issued loan with accumulated interest. Consumer credit institutions usually rely on other institutions AML/CTF procedures since the payments are made from the bank or payment institution accounts.	

Vulnerability || *Terrorist financing*	**Level: 4**
The customers of consumer credit entities are solely individual persons and 99% are residents. This makes this sector less risky in terms of TF. Consumer credit institutions are less aware of terrorist financing risks than the banking sector, resulting in cases when the purpose of credit or the leased asset is not verified.	

Mitigation measures
1. Ensure that payee's source of funds is verified as well as the customer's, if the payee differs from the client.

7.1.7. Life insurance

DESCRIPTION OF THE RISK SCENARIOS
1. A perpetrator using illicit funds pays life insurance premiums for himself / herself or employees, who are not currently employed, or for a third party.

Threat || *Money laundering*	Level: 2
Complex arrangements are required to hide the proceeds of crime in order to make life insurance a viable option for money laundering. There is a limited evidence of life insurance being used for money laundering purposes.	

Threat || *Terrorist financing*	Level: 1
No cases of life insurance contract usage for terrorist financing purposes have yet been observed. Knowledge and planning expertise are required, which dissuades terrorist groups to look for easier way to finance their activities.	

Vulnerability || *Money laundering*	Level: 2
Life insurance sector is non cash only and mainly relies on banks AML/CTF controls, especially in the area of source of funds verification. Some life insurance companies identify PEPs based on information provided by the client and do not employ any database to verify PEPs information.	

Vulnerability || *Terrorist financing*	Level: 1
Due to the low level of attractiveness of life insurance products to the terrorist groups, the TF risk exposure should be considered as low.	

Mitigation measures
1. Enhance and improve KYC and customer due diligence (CDD) processes and ensure the verification of customers' origin of funds.

7.1.8. Money remittance

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrators conduct cash transfers of low value in order to finance terrorists. 2. Perpetrators break down large amounts of cash acquired by criminal activities, thus they remain below the thresholds for required customer identification. 3. Perpetrators via money remittance agents launder illicit funds. Agents use fictitious IDs and supporting documents to launder money.

Threat || *Money laundering*	Level: 3
Due to the vast network of money remittance providers and their agents, the fact that the product does not require specific knowledge or planning, perpetrators may use the sector for money laundering purposes.	

Threat || *Terrorist financing*	Level: 3
Terrorist groups may use money remittance services to finance their activities because of the sector's broad intermediary network and product simplicity.	

Vulnerability || *Money laundering*	Level: 3
Money remittance business is mostly cash-based and allows speedy transactions. Although the value of a single transactions is usually low, aggregated it can reach significant volume of transfers. Money remittance providers do not collect the information on the source of funds and the purpose of transaction, except cases, when the client's transactional activity is meets the CDD and ECDD triggers, i.e. when the volume of transactional activity exceeds EUR 600 per one transaction or aggregated in 24 hours; EUR 15,000 in 90 days; when the medium & high risk score is assigned to the business relationship; or when consumer transactions are made to/from high risk jurisdictions.	

Vulnerability || *Terrorist financing*	Level: 3
Although according to the State Security Department, terrorism threat level remains low in Lithuania, EU terrorism trends do not have direct impact to Lithuania, however internal EU risks for terrorist attacks should be considered. Money remittance offices apply tailored transaction monitoring rules for TF prevention, perform sanctions screening, and restrict transfers related to high risk countries, such as Iran and North Korea.	

Mitigation measures
1. Ensure that the money remittance companies establish proper internal control procedures to monitor intermediaries and agents activities.

7.1.9. Payment / E-money institutions

DESCRIPTION OF THE RISK SCENARIOS
1. The business, which does not have any legitimate activity, and therefore no legitimate source of funds, performs fictitious transactions in order to disguise criminal proceeds as legitimate earnings from trade in goods and services, especially intangible services such as marketing, IT services and consulting. 2. Companies set up fictitious loans with each other to justify transfers of funds of illegal origin. 3. Perpetrator launders money by making the instant payment to/from dormant account. 4. Perpetrators use genuine accounts of money mules to process illegal payments linked to terrorism, money laundering and other economic crimes. 5. A perpetrator uses e-money account as transition account for fictitious goods and services and later transfers illicit origin funds to a bank account.

6. A perpetrator, having several passports, uses the one, which is more favorable in terms of AML/CTF, and opens the e-money account.

Threat || *Money laundering*	**Level: 3**
Payment and e-money institutions are attractive for perpetrators as in most cases KYC is performed by non-face-to-face means. Products have advantage over cash when it comes to moving money outside of Lithuania and the EU. Unlike in the case of terrorist financing, e-money is attractive for criminal organizations, since it is possible to transfer large amounts of money with a low expertise.	

Threat || *Terrorist financing*	**Level: 3**
E-money products present some advantages over cash when it comes to making online payments, and the use of these products does not require great expertise. It is sometimes easier to pay for some products or services (e.g. hotels, car rentals) using e-money products than by cash. Disadvantage of using e-money is its traceability and audit trail opportunities.	

Vulnerability || *Money laundering*	**Level: 3**
Large part of customers in the sector are non-residents, in some entities almost up to 100%, making it more difficult to verify the beneficial owner and verify the business purpose. Large part (up to 70%) of customers are from offshore countries. Supervisory authorities have identified cases with incorrect customer's or beneficial owners verifications due to the fact that it was not a face-to-face procedure (i.e. bad quality of ID's, remote identification and verification did not meet the legal acts requirements). Due to the fact that many of the clients are non-resident or from offshore countries, the companies have difficulties to identify the clients in reliable and independent sources. The applied KYC, customer due diligence and transaction monitoring systems are less effective than the ones used in the banking sector, as most of the businesses are new and focus on increasing clients' portfolio instead of AML/CTF regulatory compliance. Most institutions have not yet performed organization-wide risks assessments to identify the risks based on five factors (geographies, customers, products or services, delivery channels, other qualitative risks). Next to that, not all institutions perform the retrospective transaction monitoring. Operations in cash make only 2% of total clients' turnover in the institutions which perform operations in cash. From 2016 to 2019 number of payment and e-money institutions doubled, i.e. from 52 to 107 institutions, which might create challenges for the supervisory institutions to perform timely inspections, onsite and offsite.	

Vulnerability || *Terrorist financing*	**Level: 3**
E-money and payment institutions have a lower knowledge of TF risk and its controls than the banking sector. They also have a limited access to information which would aid in determining and monitoring the TF risk. Many of the customers are non-residents, who live in offshore countries and it is impossible to find their beneficial owners on independent sources. The systems and processes used to determined TF risk are the same as the ones applied for money laundering, as well as transaction monitoring scenarios are not set to determine TF cases. The main tool which is used to investigate the TF risk is the customer's, beneficial owners, fund senders or receivers sanction screening. However, perpetrators related to terrorism activities are usually not yet on the sanction lists. The financial sanctions target	

individuals or groups that are already known to pose a threat, whereas risk often emanates from individuals who are not caught by the sanctions regime, therefore it is not a sufficient TF risk control measure.

Mitigation measures
1. Ensure proper KYC procedures, including identification of the client and beneficial owner. 2. Tailor customer due diligence and transaction monitoring procedures to TF prevention, not only ML prevention. 3. Summarize the reports on suspicious transactions, share knowledge on specific ML/TF schemes and ensure collaboration between private and public sectors in regards to the risks. 4. Raise the knowledge of TF risk management and international financial sanctions and restriction measures in the sector. 5. Ensure that as the sector is growing, there would be sufficient resources to perform risk based supervision.

7.1.10. Virtual currencies

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrators use virtual currencies systems to transfer funds with illegal origin or purchase goods anonymously (cash funding or third party funding through virtual exchanges). 2. Terrorist groups receive anonymous funding or purchases as virtual currency (cash funding or third party funding through virtual exchanges in which the funding source is not properly identified). 3. Perpetrators use criminal money to set up a virtual currency company that deposits criminal money. 4. A perpetrator deposits or withdraws illegally obtained virtual currency in a cashpoint machine and/or use cryptocurrency card for payments.

Threat || *Money laundering*	**Level: 4**
Criminal groups may be in favor of money laundering through virtual currencies due to the ease of transferring virtual currencies to different countries, as well as the absence of homogeneous ML risk prevention measures and the high anonymity of fund transfers.	

Threat || *Terrorist financing*	**Level: 4**
Terrorists find virtual currency attractive because of its features like non-face-to-face customer relationships and anonymity of transfers.	

Vulnerability || *Money laundering*	**Level: 4**
High level of anonymity (due to the absence of customer identification processes or use of non-reliable non-face-to-face technological solutions) and speed of fund transfers enable interaction with high-risk	

areas or high-risk customers (darknet[28]), which cannot be identified. Many virtual currency providers are set up abroad what makes the traceability difficult. Major technical solutions are needed in order to identify recipients of virtual currency. Due to lack of traceability of funds, there is a struggle to evaluate the risk and scope of virtual currencies impact on money laundering scale.
The supervisory authority has its opinion on ML risk mitigation measures related to virtual currencies, but it lacks the legal framework and regulation.

Vulnerability || *Terrorist financing*	**Level: 4**
Due to the development of new technological solutions, risk of virtual currency to be used to finance terrorism is emerging. Such characteristics as internet-based operation, cross-border transfers and anonymity make virtual currency sector vulnerable and exposed to terrorists. There is a lack of data of the virtual currency sector impact on terrorist financing. This information is needed in order to raise the knowledge of TF risk in the sector.	

Mitigation measures

1. Competent authorities should monitor developments in virtual currencies sector and assess whether changes to national legal and regulatory AML/CFT frameworks are required.
2. Ensure that all virtual currency service providers meet AML/CFT requirements.
3. Regulatory authorities should assess and monitor the risks posed by blockchain technology.

7.2. Other sectors

7.2.1. Accountants, auditors and tax advisors

DESCRIPTION OF THE RISK SCENARIOS

1. Perpetrators in collaboration with accountants, auditors or tax advisors help establish and manage money-laundering schemes.
2. Accountants as collaborators do false accounting in favor of perpetrators to launder money.
3. Perpetrators in collaboration with accountants or tax advisors purchase real estate using funds with illegal origin.
4. Perpetrators in collaboration with accountants, auditors or tax advisors provide assurance and/or assistance with tax compliance, which may be unfairly performed in the interest of the perpetrator.

Threat || *Money laundering*	**Level: 4**
Criminal organizations often seek for services or even involvement of accountants, auditors or tax advisors in money laundering schemes. Risk of infiltration or ownership by organized crime groups is a money laundering threat for accountants, auditors and tax advisors.	

Threat || *Terrorist financing*	**Level: 3**

[28] Darknet is a computer network with restricted access that is used mostly for anonymous and illegal peer-to-peer file sharing.

The assessment of the terrorism threat has been analyzed together with money laundering schemes provided by accountants, auditors and tax advisors. However, no such cases have yet been observed.

Vulnerability || *Money laundering*	**Level: 3**

Accountants, auditors and tax advisors could easily be involved in money laundering schemes because most of their services are used for legitimate purposes. Regulation and strict ethical and professional rules are applied to these professionals. However, strong organizational framework at EU level might not enable each professional to be adequately aware of ML risks and follow the regulation. The sector in Lithuania is small and has low level of awareness of money laundering risk and related schemes. There are indications of weaknesses in the way accountants, auditors and tax advisors carry out checks and manage risks, especially in situations of irregular or one-time service, when the professionals carry out their tasks without having a full understanding of their customer's, who mostly are residents, financial situation. Although there are not many non-resident clients, similarly to the sectors mentioned before, accountants, auditors and tax consultants are unable to perform sanctions screenings, investigate PEPs and verify beneficial owners in proper databases.

Vulnerability || *Terrorist financing*	**Level: 2**

Based on State Security Department of Lithuania data, due to the geographical location, low number of different ethnic groups, the potential of services of accountants, auditors and tax advisors to be used by terrorists is very limited. Although small part of the customers are non-residents, the sector still fails systematically perform checks on sanctions and PEPs, and determine the ultimate beneficial owner. There is no systematical, all auditors applicable resolution of national information systems and operative information extraction from registers in relation to client's or beneficial owner's verification.

Mitigation measures

1. Ensure that accountants, auditors and tax advisors accurately apply AML/CFT requirements.
2. Provide guidance and better understanding on risk factors for external accountants, auditors and tax advisors.
3. The Lithuanian Chamber of Auditors should initiate data provision contracts to the auditors, where the information would come from the state registry (JADIS and JAR), which would ensure a reliable and independent source of data.

7.2.2. Advocates

DESCRIPTION OF THE RISK SCENARIOS

1. Advocates help perpetrators to set up a fictitious legal entity and create complex corporate ownership structures involving many legal entities associated with high ML/TF risk jurisdictions.
2. Perpetrators in collaboration with advocates establish and manage money-laundering schemes.
3. A perpetrator with a help of advocate uses advocate's deposit account to receive and transfer funds for the money laundering purpose.

Threat || *Money laundering*	Level: 4
Knowledge of domestic and international regulatory and taxation rules is required to establish corporate structures that may be used for money-laundering purposes, which can be provided only by professional intermediaries. Therefore, perpetrators target advocates. Perpetrators find advocate services beneficial for the money laundering purpose because they can create complex chains of ownership throughout different countries. The usage of "shell companies" for money laundering seem to be very attractive for criminals since they can open and use bank account for fictitious purchases of goods and services; business could be set up online and preserve the identities of their owners.	

Threat || *Terrorist financing*	Level: 4
Because high level of technical expertise and knowledge is required, terrorists might use advocate service but due to its complexity, terrorist groups might find easier ways to finance their activities. No such cases have yet been observed.	

Vulnerability || *Money laundering*	Level: 4
Advocates are able to create legal entities remotely and make the process fully anonymous. Some advocates are not aware of actual purpose for which the established company is used, and therefore do not consider themselves as collaborators in these ML schemes. However, some advocates may provide dedicated services to hide the beneficial ownership with a purpose of assisting in setting up money laundering schemes, which most of them are known. There is a weak control in place and advocates are failing in their duty to report suspicious activities. In 2016-2018, advocates submitted no suspicious transaction reports. Most advocates do not perform comprehensive customer due diligence and do not employ related monitoring systems.	

Vulnerability || *Terrorist financing*	Level: 3
Knowing that legal entities could be created remotely and fully anonymous, terrorist groups could misuse advocates to create a corporate structure with no legitimate purpose. However, some advocates may provide dedicated services to hide the beneficial ownership of their customers with a purpose of setting up terrorist financing schemes. The risk that these structures could be used to hide the beneficial owner is well known. Although legal professionals in Lithuania are subject to EU anti-money laundering requirements, supervisory authorities are not always able to deliver proper guidance to this sector.	

Mitigation measures

1. Provide training sessions and guidance on risk factors with a focus on non-face-to-face business relationships, offshore professional intermediaries and customers with complex/shell structures.
2. Discuss and evaluate the possibility to prohibit establishment of shell structures.
3. Prepare annual reports on the measures taken by advocates to comply with their customer due diligence obligations, including beneficial ownership requirements, suspicious transaction reports and other internal controls.
4. Ensure that the information used for identifying beneficial owner is regularly reviewed and updated.

7.2.3. Notaries

DESCRIPTION OF THE RISK SCENARIOS
1. A perpetrator uses notary's deposit account to receive and transfer funds for the money laundering purpose. 2. Counterparties settle some part of transaction in cash before going to notary and at a notary they formalize deal for a smaller amount for which transaction is made. 3. A perpetrator at notary formalize the purchase price higher than the market value. 4. When performing operations at notary, an individual client is being controlled by other individual person or group of persons for criminal purposes.

Threat || *Money laundering*	**Level: 4**
Criminal organizations use notary services such as confirmation of company registration documents and contracts, as well as money deposits into deposit accounts, in order to perform money laundering operations by concealing the source of funds.	

Threat || *Terrorist financing*	**Level: N/A**
Not relevant.	

Vulnerability || *Money laundering*	**Level: 3**
According to the Lithuanian regulations the ownership transfer of real estate, except transfer due to the bankruptcy cases, must be performed through notaries. Such ownership transfer of real estate often involve payments in cash, except for the purchases of land for agricultural purposes. Thus the notaries are exposed to the same risks as defined under trade in goods in cash. Some of the notaries do not perform additional research to determine source of funds or the assets related to their performed operations of the clients. These notaries accept written confirmations on the source of funds provided by clients, but do not verify the information themselves. In addition, it is difficult to determine whether all notaries perform checks of the clients and their business partners in PEP and sanctions databases, statistics is not collected. Because the notary does not have a business relationship with its clients, monitoring of business relationship is not performed.	

Vulnerability || *Terrorist financing*	**Level: N/A**
Not relevant.	
Mitigation measures	
1. Set limits on the use of cash by introducing the ceiling amount for cash payments. 2. Provide training sessions and guidance on risk factors with a focus on AML/CTF compliance. 3. Prepare annual reports on the measures taken by notaries to verify how notaries identify beneficial owner according to documentation and information from a reliable and independent source; how suspicious transactions reports are prepared and what other internal controls are applied in ML / TF prevention area.	

7.2.4. Bailiffs

DESCRIPTION OF THE RISK SCENARIOS
1. In return for obtaining illegal origin cash, the indebted gives property to a perpetrator and use the money to pay off the debt to the bailiff. 2. A bailiff states factual circumstances of assets held by a perpetrator or its close relative.

Threat || *Money laundering*	**Level: 3**
Money-laundering structures using bailiffs could be possible with or without their awareness. Perpetrators could target bailiffs or their debtors because they can be intermediaries in money-laundering schemes.	

Threat || *Terrorist financing*	**Level: N/A**
Not relevant.	

Vulnerability || *Money laundering*	**Level: 1**
In 2016-2018 bailiffs provided only four STRs, which could propose that not all bailiffs follow the AML/CTF requirements. Some bailiffs do not perform monitoring of business relationship with their clients, stating that they do not establish business relationships. The supervisory authorities have paid a sufficient amount of attention to the bailiffs sector and have performed yearly reviews of the sector. Many bailiffs do not accept payments in cash and amounts of cash operations are rather small. The largest part of the transactions come from debtors settlement accounts registered in Lithuania.	

Vulnerability || *Terrorist financing*	**Level: N/A**
Not relevant.	

Mitigation measures
1. Provide training sessions and guidance on risk factors with a focus on AML/CTF compliance. 2. Prepare annual reports on the measures taken to verify bailiffs' compliance with their customer due diligence obligations, monitoring system requirements, suspicious transaction reports and internal controls.

7.2.5. Non-profit organizations

7.2.5.1. Religious organizations

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrators donate to religious organizations, which may fund terrorists.

2. A perpetrator establishes religious organization for money laundering and/or terrorist financing purposes.

Threat || *Money laundering*	**Level: 2**
Perpetrators find religious organizations attractive for money laundering purposes because religious organizations accept anonymous donations in cash and do not have obligation to prove the usage of funds.	

Threat || *Terrorist financing*	**Level: 2**
Organized terrorist groups may infiltrate religious organizations to fund foreign terrorist fighters. They find religious organizations related to their target country very attractive, because it allows cross-border activities.	
Vulnerability || *Money laundering*	**Level: 3**
Religious organizations are not obliged entities under the AML/CTF Law. Since it is possible to accept anonymous donations in cash freely and there is no obligation to prove the usage of funds, it is difficult to exercise control of the use of the targeted donations as well as general control of religious organisation financing (transparency and legitimacy).	

Vulnerability || *Terrorist financing*	**Level: 3**

Majority (more than 90%) of citizens in Lithuania are Christians or non-believers.
At the end of the year 2018, there were 1,312[29] religious communities, associations or other religious organizations registered and included in the Register of Legal Entities, including 1,118 traditional religious organizations and 194 non-traditional religious organizations.

Religion	**Number of religious organizations registered in 2018**
Roman Catholics	900
Other Christian origin religions	360
Judaism religions	10
Islamic religions	12
Hindu religions	6
Buddhist religions	13
Other religions (Bahá'í, Karaites, Pagans)	11

Mitigation measures

1. Establish strong financial management, including having robust internal and financial controls and risk management procedures.
2. Carry out proper due diligence on those individuals and organizations which make monetary operations or work closely with religious organizations.

[29] Ministry of Justice of the Republic of Lithuania https://tm.lrv.lt/lt/veiklos-sritys-1/religiniu-bendruomeniu-ir-bendriju-reguliavimas/religiniu-bendruomeniu-ir-bendriju-registravimas

3. Carry out due diligence on partners, especially those who operate in a close proximity to an active terrorist threat.

7.2.5.2. Charities

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrators donate to charities, which are not accountable for usage of funds. 2. A perpetrator establishes charity for money laundering and/or terrorist financing purposes. 3. Charity or its directing officials knowingly or unknowingly maintains an affiliation with a terrorist entity which may result in the charity being abused for multiple purposes, including general logistical support to the terrorist entity. 4. Charity supports terrorist groups with legitimate resources at the point of delivery. 5. A perpetrator, as an actor inside the charity or external actor (such as foreign partner or third-party fundraiser), using the diversion of funds method, supports terrorist entities at some point through the charity's operational or financial processes. 6. Charity supports recruitment of terrorist entities. 7. Terrorist entities falsely represent themselves as the agents of charity in order to deceive donors into providing support.

Threat || *Money laundering*	**Level: 2**
Perpetrators find charities attractive for money laundering purposes because charities accept anonymous donations in cash and do not have obligation to prove the usage of funds.	

Threat || *Terrorist financing*	**Level: 2**
Organized terrorist groups may infiltrate charities to fund foreign terrorist fighters. There is a stronger risk of abuse for charities providing service activities "in close proximity to an active terrorist threat" (conflict of target areas). Terrorists find charities with a purpose (humanitarian etc.) related to their target country very attractive, because it allows cross-border activities. The charities most at risk of abuse for terrorist financing are engaged in "service activities", meaning programs focused on providing housing, social services, education, or health care.	

Vulnerability || *Money laundering*	**Level: 3**
Charities in Lithuania are not obliged entities under the AML/CTF Law. Since it is possible to accept anonymous donations freely and there is no obligation to prove the usage of funds, it is difficult to exercise general control of the use of targeted donations and general control of financing transparency and legitimacy of the financing of the charities.	

Vulnerability || *Terrorist financing*	**Level: 3**
Charities in Lithuania are not obliged entities under the AML/CTF Law. It is possible to accept anonymous donations freely and there is no obligation to prove the usage of funds.	

Mitigation measures
1. Establish strong financial management, including having robust internal and financial controls and risk management procedures. 2. Carry out proper due diligence on those individuals and organizations that give money to, receive money from or work closely with the charities. 3. Carry out due diligence on partners, especially those who operate in a close proximity to an active terrorist threat. 4. Strengthen charities' self-regulation to promote greater transparency and good governance within the larger NPO sector. Charities without self-regulatory mechanisms could consider the development of their own or additional self-regulatory mechanisms to strengthen internal controls and procedures, due diligence and other measures to improve transparency of their operations and funding and to prevent terrorism and other abuses.

7.2.6. Gambling sector

7.2.6.1. Product: Casinos (A category)

DESCRIPTION OF THE RISK SCENARIOS
1. A perpetrator or his / her collaborator purchases casino chips using illicit cash and at the end of a game converts it back to cash or receives transfer to his / her account. 2. A perpetrator buys casino chips using illicit cash from other customers and receives a win statement. 3. Organized crime groups open a casino themselves or infiltrate to launder money.

Threat || *Money laundering*	Level: 4
Casino sector is exposed to the risk of infiltration or ownership, because the activity based on significant number of cash flows is attractive for organized crime groups, PEPs and those coming from high-risk countries to launder money. Modus operandi is easy to implement as it requires basic planning and basic knowledge of how gambling system work.	

Threat || *Terrorist financing*	Level: N/A
Not relevant.	

Vulnerability || *Money laundering*	Level: 3
Casinos allow only cash operations and do not verify the source of funds. In addition, the sector has difficulties in performing customer due diligence (no evidence that all casinos would employ systems to identify related transactions of players), sanctions checks and PEPs identification. Also, some casinos have customers from sanctioned or high-risk countries, such as Iran and Syria. However, casinos are the most aware of money laundering risks in comparison with other gambling sectors. The number of investigations carried out by supervisory authorities during 2016-2018 is insufficient and not proportional to the risk of the sector. This might be caused by the lack of human resources of the supervisory authority, which has only three employees dedicating only 15% of their time for ML / TF supervision within the sector.	

All tables and chips inventory counts in casinos are filmed in HD format and the videos are saved for 180 days. Each day the inventory count data is provided to the supervisory authority.
The slot machines in casinos have a counter, which makes it difficult to show fictitious income. In two years, all slot machines in casinos will be connected to one live system, which will be monitored by the supervisory authority.

Vulnerability || *Terrorist financing*	**Level: N/A**
Not relevant.	

Mitigation measures

1. Allow the use of debit cards in order to reduce the amount of cash.
2. Set limits on the use of cash by introducing the maximum amount allowed per person at a defined period.
3. Promote player cards, devices used by gambling services providers to track the time and amount of bets played by the players, to ease customer identification and limit the use of cash.
4. Supervisory authorities should conduct sufficient number on-site inspections depending on the risk and progress in AML/CTF compliance. “Secret shopper” method should be also employed.
5. Support the sector with annual trainings tailored to casino industry, guidance on customer due diligence and implementation of AML/CFT requirements. The sector itself should pay more attention to increasing self-awareness related to ML/TF related schemes and prevention.
6. Prepare annual reports on the measures taken to verify casinos’ compliance with their customer due diligence obligations, beneficial owners’ verifications, monitoring system requirements, suspicious transactions reports and internal controls to ensure that sector complies with AML/CTF requirements.
7. Supervisory authorities should provide feedback on the STRs submitted by lottery operators in order to improve quality of reporting and the usage of reported information.

7.2.6.2. Product: Gaming machines (B category)

DESCRIPTION OF THE RISK SCENARIOS

1. Organized crime groups establish fictitious gaming machines business.
2. A perpetrator plays using illicit cash and receives a win statement or withdraws cash by inputting illicit funds to a slot machine.

Threat || *Money laundering*	**Level: 3**
Gaming machines (land-based), as a product, are exposed to the risk of infiltration or ownership. However, because of low amounts of winnings, other gambling products could be more attractive than gaming machines.	

Threat || *Terrorist financing*	**Level: N/A**
Not relevant.	

Vulnerability || *Money laundering*	Level: 3
The sector is cash based only. Players are not identified for ML / TF purposes when played up to €1,000; however, the sector does not have a system which allows to monitor the related transactions. The machines have a counter, which makes it difficult to show fictitious income. The cashier and entrance are filmed in HD format and the videos are saved for 180 days. In two years, all gaming machines will be connected to one live system, which will be monitored by the supervisory authority.	

Vulnerability || *Terrorist financing*	Level: N/A
Not relevant.	

Mitigation measures

1. Allow the use of debit cards to reduce the amount of cash.
2. Set limits on the use of cash by introducing the maximum amount allowed per person at a defined period.
3. Promote player cards, devices used by gambling services providers to track the time and amount of bets played by the players, to ease customer identification and limit the use of cash.
4. Support the sector with annual trainings tailored to the industry and guidance on customer due diligence and implementation of AML/CFT requirements. The sector itself should pay more attention to increasing self-awareness related to ML/TF related schemes and prevention.
5. Supervisory authorities should conduct sufficient number on-site inspections depending on the risk and progress in AML/CTF compliance. “Secret shopper” method should be also employed.
6. Prepare annual reports on the measures taken to verify gaming machines sector compliance with their customer due diligence obligations, beneficial owners’ verifications, monitoring system requirements, suspicious transactions reports and internal controls to ensure that sector complies with AML/CTF requirements.
7. Supervisory authorities should provide feedback on the STRs submitted by lottery operators in order to improve quality of reporting and the usage of reported information.

7.2.6.3. Product: Betting

DESCRIPTION OF THE RISK SCENARIOS

1. A perpetrator creates fixed matches schemes.
2. A perpetrator launders money by betting for the guaranteed win (very probable outcome) in order to revolve illicit money through betting and claim it as a win (conversion).
3. An organized crime group starts betting business to launder money by setting fictitious bets.
4. A perpetrator purchases winning tickets from other players using illicit funds with intent to launder money.

Threat || *Money laundering*	Level: 3
Betting sector is exposed to the risk of organized crime groups’ infiltration into the sector through the ownership of betting agencies and/or direct involvement in betting activity. To remain concealed, the true beneficial owners (associated with higher ML risk – e.g. PEPs and those coming from high ML risk	

countries) may hide their identity and stay anonymous by using third parties to register and receive the winnings in their interest. Fast and high volume money transfers / conversion, make the betting activities attractive for those who intend to be engaged in money laundering activities.

Threat || *Terrorist financing*	**Level: N/A**
Not relevant.	

Vulnerability || *Money laundering*	**Level: 3**
Land-based betting activities are cash based. Due to none submitted STRs and CTRs, the sector may be considered not fully aware of money laundering risks. The sector has difficulties in monitoring related transactions as the legislation does not require to perform customer identification when the payment is up to €1,000. Player cards, equally as winning tickets are anonymous, i.e. not personalized. Cash (given by a player) calculation by a cashier as well as customer's entrance is filmed in HD format and the video is saved for 180 days.	

Vulnerability || *Terrorist financing*	**Level: N/A**
Not relevant.	

Mitigation measures

1. Allow the use of debit cards to reduce the amount of cash.
2. Set limits on the use of cash by introducing the maximum amount allowed per person at a defined period.
3. Promote personalized player cards.
4. Supervisory authorities should conduct sufficient number on-site inspections depending on the risk and progress in AML/CTF compliance. "Secret shopper" method should be also employed.
5. Support the sector with annual trainings tailored to the industry and guidance on customer due diligence and implementation of AML/CFT requirements. The sector itself should pay more attention to increasing self-awareness related to ML / TF related schemes and prevention.
6. Prepare annual reports on the measures taken to verify betting operators' compliance with their customer identification and due diligence obligations, beneficial owner verification procedures, monitoring system requirements, suspicious transaction reports and internal controls to ensure that sector complies with AML/CTF requirements.
7. Supervisory authorities should provide feedback on the STRs submitted by lottery operators in order to improve quality of reporting and the usage of reported information.

7.2.6.4. Product: Lotteries

DESCRIPTION OF THE RISK SCENARIOS

1. A perpetrator purchases a lottery ticket from the winner using illicit funds.
2. An organized crime group starts lottery business to launder money.

Threat || *Money laundering*	Level: 2
Lottery sector is exposed to the risk of organized crime groups' infiltration into the sector through the ownership of lottery organizers and/or direct involvement in lottery activity. However, lotteries as a money-laundering channel are not attractive to criminals due to the low frequency of draws, low average stakes and winnings, which give fewer opportunities to launder money.	

Threat || *Terrorist financing*	Level: N/A
Not relevant.	

Vulnerability || *Money laundering*	Level: 2
According to the obtained statistical data, no CTRs, STRs were submitted to competent authorities by the sector during the period of 2016-2018. It is impossible to control that winning tickets, which are not personalized, would not be sold to perpetrators. Customer identification is performed only if winning exceeds €1,000.	

Vulnerability || *Terrorist financing*	Level: N/A
Not relevant.	

Mitigation measures
1. Support the sector with annual trainings tailored to casino industry and guidance on customer due diligence and implementation of AML/CFT requirements. 2. Prepare annual reports on the measures taken to verify lottery operators' compliance with their customer identification and due diligence obligations, suspicious transaction reporting and the level of internal controls to ensure that the sector complies with AML/CTF requirements. 3. Supervisory authorities should provide feedback on the STRs submitted by lottery operators in order to improve quality of reporting and the usage of reported information.

7.2.6.5. Product: Online gambling

DESCRIPTION OF THE RISK SCENARIOS
1. A facilitator ("money mule") gives his / her account to perpetrator to engage in online gambling activity in order to launder money. Crime organizations may purchase online casino accounts containing funds already uploaded by non-criminal players at a higher price than the real ones. 2. An organized crime group starts online gambling business to launder money. 3. A perpetrator uses gambling sites to deposit illicit funds and to request the payout of winnings or remaining balance without engaging in gambling activity. 4. Crime organizations may use several "smurfs" to gamble online directly against each other using illicit funds. One of the "smurfs" receives all the funds as a winner, and withdraws the funds as the legitimate gambling earnings.

5. Crime organizations invent and bet online on fictitious (non-existing) matches or events to ensure winnings.

Threat || *Money laundering*	**Level: 3**
Online gambling sector is exposed to the risk of organized crime groups' infiltration into the sector through the ownership of online gambling organizers and/or direct involvement in lottery activity. This industry is attractive for ML due to the high volume and fast execution of transactions (including cross-border) as well as low identification requirements, which allows to easily convert illegal funds into legitimate gambling earnings.	

Threat || *Terrorist financing*	**Level: N/A**
Not relevant.	

Vulnerability || *Money laundering*	**Level: 2**
The awareness of the risk reflects in high number of inspections carried out by the supervisory authority in 2016-2018. Sector is not homogenous; some online gambling operators have stricter AML/CTF compliance procedures than others do. As all gaming is done online, where a good audit trail exists. Identification is performed for all players despite the amount played; however, verification of source of funds does not exist as the sector relies on banks and other payment institutions (the sector is no cash only).	

Vulnerability || *Terrorist financing*	**Level: N/A**
Not relevant.	

Mitigation measures

1. On regular basis support the sector with trainings tailored to online gambling industry and guidance on customer identification, due diligence and implementation of AML/CFT requirements.
2. Prepare annual reports on the measures taken to verify online gambling operators' compliance with their customer identification and due diligence obligations, suspicious transaction reports and internal controls to ensure that the sector complies with AML/CTF requirements.
3. Supervisory authorities should provide feedback on the STRs submitted by online gambling operators in order to improve quality of reporting and the usage of the reported information.
4. Assess cyber security risks of online gambling to support detection and prevention of money laundering activities.

7.2.7. Trade in precious stones and precious metals

DESCRIPTION OF THE RISK SCENARIOS
1. A perpetrator purchases precious stones or precious metals using illegal cash. 2. Terrorists or their collaborators sell the precious stones or precious metals obtained through robberies to finance terrorist activities.

Threat || *Money laundering*	Level: 4
Criminals favor precious metals and precious stones, such as gold and diamonds, because they are easy to store and turn into cash.	

Threat || *Terrorist financing*	Level: 3
Proceeds of the sale from high value assets may be used to finance criminal operations. Especially precious stones and gold is very attractive to terrorist groups in conflict zones, because it is easy to move them across borders and it is financially viable option.	

Vulnerability || *Money laundering*	Level: 3
Up to 80% of deals in high value assets, trading companies were made using cash. The weak point of the sector that it is not compliant with AML/CTF requirements. Sellers do not obtain information and assess the source of funds, do not perform PEP/sanctions/adverse media screening. No STRs were submitted in 2016-2018 and only one jewelry reported CTRs during this period.	

Vulnerability || *Terrorist financing*	Level: 3
The same vulnerabilities apply for terrorist financing as for money laundering.	

Mitigation measures
1. Conduct sufficient unannounced spot checks at diamond companies and gold traders to identify possible loopholes in compliance with customer due diligence requirements and involve sector experts to check the flow of goods. 2. Support the sector with trainings on customer due diligence and other AML/CFT requirements. 3. Set limits on the use of cash by introducing the maximum amount allowed for cash payments.

7.2.8. Trade in movable cultural goods and antiques

DESCRIPTION OF THE RISK SCENARIOS
1. A perpetrator purchases movable cultural goods and antiques using illegal cash. 2. Terrorists or their collaborators sell the antiques and other cultural goods obtained through robberies, to finance terrorist activities.

Threat || *Money laundering*	**Level: 3**
Criminals favor to purchase movable cultural goods and antiques using cash money obtained in illegal activities. However, it takes some knowledge to later sell the goods for the best price.	

Threat || *Terrorist financing*	**Level: 3**
Proceeds of the sale from high value assets may be used to finance criminal operations. In addition, such asset is a profitable source of finance.	

Vulnerability || *Money laundering*	**Level: 3**
Up to 80% of deals in high value assets, trading companies were made using cash. The weak point of the sector that it is not compliant with AML/CTF requirements. Sellers do not obtain information and assess the source of funds, do not perform PEP/sanctions/adverse media screening.	

Vulnerability || *Terrorist financing*	**Level: 3**
The same vulnerabilities apply for terrorist financing as for money laundering.	

Mitigation measures
1. Conduct sufficient unannounced spot checks at antique shops to identify possible loopholes in compliance with customer due diligence requirements and involve sector experts to check the flow of goods. 2. Support the sector with trainings on customer due diligence and other AML/CFT requirements. 3. Set limits on the use of cash by introducing the maximum amount allowed for cash payments.

7.2.9. Trade in goods in cash

DESCRIPTION OF THE RISK SCENARIOS
1. Perpetrator converts laundered criminal proceeds into assets such as vehicles, yachts and other valuable assets. 2. Perpetrators open cash-based business or collaborate with the cash based business owners to infiltrate illegal cash into the financial system based on fictitious economic activities. 3. Terrorist groups might run cash-intensive business to launder money and / or sell high-value goods such as antiques and jewelries and use these funds to finance terrorist activities.

Threat || *Money laundering*	**Level: 4**
Cash is the preferred option for criminals, which allows hiding illicit proceeds of crime and moving funds rapidly. It could be considered as one of the easiest way to hide illegitimate proceeds of crime as the modus operandi does not require specific expertise, knowledge or planning capacities. Motor vehicles are one of the main target goods because of their high value and demand. Perpetrators may buy motor vehicles using illegal cash specifically where restrictions on cash payments are limited, for example on second-hand vehicle market.	

Threat || *Terrorist financing*	**Level: 4**
Terrorist groups frequently use cash in making required purchases, as cash is attractive, almost impossible to detect and does not require specific expertise to be used.	

Vulnerability || *Money laundering*	**Level: 4**
Cash intensive businesses allow speedy and anonymous transactions. Risk awareness of sectors not covered by AML/CFT obligations is low; sellers do not assess the source of funds and do not perform PEP/sanctions/adverse media screening of their clients. Some customers are non-residents, especially in the case of second-hand vehicle market. No cash limitations are defined in local legislation, which makes Lithuania more vulnerable than other countries in EU having such limitations. In 2016-2018 up to 33% of deals in motor vehicle companies were made in cash. However, this number could be much higher in second-hand vehicle market as the official statistics does not exist.	

Vulnerability || *Terrorist financing*	**Level: 4**
The sector shows the same vulnerability to TF as to ML.	

Mitigation measures
1. Set limits on the use of cash by introducing the maximum amount allowed for cash payments. 2. Provide training sessions and guidance on risk factors with a focus on AML/CTF compliance. 3. Perform continuous monitoring on how AML/CTF obligations are implemented and prepare annual reports on the measures taken. Verify that dealers, participating in transactions over €10000, comply with regulatory requirements.

7.2.10. Trade in real estate

DESCRIPTION OF THE RISK SCENARIOS
1. A perpetrator purchases real estate using illegally obtained cash.

Threat || *Money laundering*	**Level: 4**
The real estate sector is often used in combination with notary sector for money laundering purpose. The real estate scheme does not require specific expertise or knowledge, which is an attractive characteristic for the perpetrator.	

Threat || *Terrorist financing*	**Level: 4**
Terrorist or a facilitator could obtain real estate using illegal cash and later sell it or rent it out to finance terrorist activities. Often legal professionals are intermediaries to facilitate the acquisition of real estate.	
Vulnerability || *Money laundering*	**Level: 4**
In Lithuania, still a large part of the real estate purchases are made in cash.	

Majority of real estate agents, which are obliged entities under the AML/CTF Law, do not perform customer due diligence and do not check the origin of funds, PEPs, sanctions and other information in databases relevant to AML/CTF requirements.
The real estate sector is not homogeneous and not well organized to be evenly aware of the money laundering risks. Nevertheless, the money-laundering scheme of using real estate is well known.

Vulnerability || *Terrorist financing*	**Level: 4**
The same vulnerabilities apply for terrorist financing as for money laundering.	

Mitigation measures

1. Prepare annual reports on the measures taken to verify real estate' compliance with their customer due diligence obligations, suspicious transaction reports and internal controls to ensure that sector complies with AML/CTF requirements.
2. Support the sector with trainings and guidance on customer due diligence and AML/CFT requirements.
3. Set limits on the use of cash by introducing the maximum amount allowed for cash payments.

Annex 1. NRA methodology

THE METHODOLOGY FOR THE NATIONAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING

CHAPTER I
GENERAL PROVISIONS

1. The Methodology for the National Risk Assessment of Money Laundering and Terrorist Financing (hereinafter – the Methodology) was prepared in compliance with the assessment methodology of the risks of money laundering and terrorist financing affecting the internal market of the EU approved by the European Commission and it determines methods and procedures for setting the risk identification of the national money laundering and terrorist financing, assessment and risk mitigation measures (hereinafter – general risk assessment or NRA), performed in compliance with Article 28 of the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (hereinafter – the Law).
2. Terminology used in the Methodology:
   2.1. **Threat** – a person or group of people, object or activity with the potential to cause harm to financial system, public security. In the context of money laundering (hereinafter – ML) and terrorist financing (hereinafter – TF, jointly – ML/TF), this includes attractiveness (the known use of success or failure of a specific threat for ML/TF purposes) and the ability for criminals to use a specific threat to legalize property resulting from criminal activities or to finance, sponsor terrorist activities.
   2.2. **Vulnerability** – the entirety and effectiveness of legal measures, controls to prevent the realization of the threat, taking into account the extent and perception of the threat. In the ML/TF risk assessment context, looking at vulnerabilities as distinct from threat means focusing on, for example, the factors that represent weaknesses in AML/CFT systems or controls or certain features of a country. They may also include the features of a particular sector, a financial product or type of service that make them attractive for ML or TF purpose.
   2.3. **Risk** – the ability of a threat to exploit the vulnerability of a sector, products and services for the purpose of money laundering and terrorist financing.
   2.4. **Sector** – a group of professions and categories of undertakings (financial or non-financial) that may be misused for the purpose of ML/TF. This definition covers at least the following entities:
      a) financial institutions;
      b) auditors and audit companies;
      c) accounting or tax advisory firms;
      d) notaries, notary representatives, legal professionals and legal assistants, when they participate, whether by acting on behalf of and for their client in any financial or immovable property transaction, or by assisting in the planning or carrying out of transactions for their client concerning the buying and selling of immovable property or business entities; managing of client money, securities or other assets; opening or management of bank, savings or securities accounts; organisation of contributions necessary for the creation, operation or management of companies; creation, operation or management of trusts, companies, foundations, or similar legal arrangements;
      e) trust or company service providers or administrative service providers;

f) estate agents;
g) natural or legal persons engaged in commercial activities involving the trade in precious stones, precious metals, movable cultural property, antiques or other asset, to the extent that payments are made or received in cash in an amount of EUR 10 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
h) providers of gambling services.

2.5. Other terminology used in the Methodology shall be consistent with the one used in the Law.

3. NRA (see Annex 1 to the Methodology) consists of three main stages:
   3.1. risk identification;
   3.2. risk assessment;
   3.3. identification of risk mitigation measures.
4. NRA is conducted based on NRA framework (see Annex 2 to the Methodology).
5. NRA is carried out by authorities established by the Law responsible for the implementation of measures to prevent money laundering and / or terrorist financing by coordinating their actions. The authorities referred to in Article 4 (1) to (8) of the Law shall follow *mutatis mutandis* the following methodology for the risk assessment of money laundering and / or terrorist financing in a sector. Risk assessment of money laundering and / or terrorist financing in the sector is an integral part of NRA.

CHAPTER II
RISK IDENTIFICATION

6. Risk identification stage should be intended as defining a list of known and suspected ML/TF threats along with the related sectors, products, services exploited or may be exploited by criminals to perpetrate ML/TF activities. Risk scenarios are also determined at this stage.
7. When identifying risks, data and information are collected from:
   7.1. Ministry of the Interior of the Republic of Lithuania;
   7.2. Ministry of Justice of the Republic of Lithuania;
   7.3. Ministry of Finance of the Republic of Lithuania;
   7.4. Ministry of the Economy and Innovation of the Republic of Lithuania;
   7.5. Ministry of Foreign Affairs of the Republic of Lithuania;
   7.6. General Prosecutor Service;
   7.7. National Courts Administration;
   7.8. Customs department under the Ministry of Finance of the Republic of Lithuania;
   7.9. Police Department under the Ministry of the Interior of the Republic of Lithuania;
   7.10. Special Investigation Service of the Republic of Lithuania;
   7.11. State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania;
   7.12. State Security Department of the Republic of Lithuania;
   7.13. Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania;
   7.14. State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania;
   7.15. Bank of Lithuania;
   7.16. Gaming Control Authority under the Ministry of Finance of the Republic of Lithuania;
   7.17. Lithuanian Bar Association;
   7.18. Lithuanian Chamber of Notaries;
   7.19. Lithuanian Chamber of Auditors;
   7.20. Chamber of Judicial Officers of Lithuania;

7.21. Lithuanian Assay Office;
7.22. Department of Cultural Heritage under the Ministry of Culture of the Republic of Lithuania;
7.23. At least 10 (if any) private sector representatives and professional associations (if any) from all business and professional sectors involved in ML / TF prevention.

8. At least the following information is used when assessing the information:
8.1. Lithuanian legislation, guidelines and recommendations regulating ML/TF prevention;
8.2. International legislation, guidelines and recommendations regulating ML/TF prevention;
8.3. The results of a EU-wide risk assessment of money laundering and terrorist financing conducted by the European Commission and recommendations to the member states of the European Union on appropriate measures to mitigate the identified risks;
8.4. The results and recommendations of the assessment of Lithuania by the Committee of Experts of the Council of Europe on measures against money laundering and terrorist financing (Moneyval);
8.5. The results of the most recent National Money Laundering and Terrorist Financing Risk Assessment of the Republic of Lithuania and the measures applied to reduce the identified risk;
8.6. Activity reports, data and information submitted by the authorities referred to in Clause 7 of the Methodology;
8.8. Supervisory authority's statistics on the size and importance of a sector, including the number and economic importance of entities and persons in each sector;
8.9. Data on the human and financial resources allocated to the supervisory authorities for the prevention of money laundering and / or terrorist financing;
8.10. Data of the supervisory authorities on the number of supervisory actions and sanctions imposed for violations of law per year.
8.11. The number of registered criminal offenses of the legalization of proceeds of crime or the financing and sponsorship of terrorist activities, suspects, accused persons, convicted persons per year of legalization of proceeds of crime or financing and sponsorship of terrorist activities; data on the primary crimes (offenses when the property has been legalized or attempted to be legalized), if such information is available; property which has been subject to a temporary restriction of the ownership rights, its value, the property confiscated by a court decision, its value;
8.12. Number of reports of suspicious monetary operations or transactions;
8.13. NRA questionnaire responses from institutions, financial institutions and other obligated entities, professional associations referred to in Clause 7 of the Methodology, interview answers;
8.14. Information published on national and international media;
8.15. Lithuanian economic, geographical, political and legal environment.

9. Depending on the information collected, one or more of these methods, if possible, shall be used to identify the risk:
9.1. Brainstorming is used by experts for the purpose of gathering and listing as many ideas as possible. 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;
9.2. Delphi technique 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;

9.3. 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;

9.4. Assumption techniques imply testing the accuracy, instability or inconsistency of assumptions, hypotheses and what-if scenarios, which will help the assessor identifying risks.

10. When conducting NRA, the information being assessed may be subject to update at any stage of NRA.

CHAPTER III
RISK ASSESSMENT

11. When conducting the risk assessment, it is considered that ML/TF has a lasting negative impact and significant damage to the financial system, public security, and therefore risk impact (consequences) is always considered high and its value is not assessed individually.
12. When conducting the risk assessment, the threat and vulnerability related with the identified risk is being analysed.
13. The threat is determined on a scale from 1 to 4 (see Annex 3 to the Methodology):
    13.1. lowly significant (value: 1);
    13.2. moderately significant (value: 2);
    13.3. significant (value: 3);
    13.4. very significant (value: 4).
14. The vulnerability is determined on a scale from 1 to 4 (see Annex 4 to the Methodology):
    14.1. lowly significant (value: 1);
    14.2. moderately significant (value: 2);
    14.3. significant (value: 3);
    14.4. very significant (value: 4).
15. The risk level is ultimately determined by combination between the threat versus vulnerability. The risk matrix determining this risk level is based on a weighting of 40 % (threat)/ 60 % (vulnerability) - assuming that the vulnerability component has more capacity in determining the risk level. It is assumed that the level of vulnerability is likely to increase the attractiveness and hence the intent of criminals/terrorists to use a given modus operandi – thus affecting ultimately the level of threat.
16. The level of risk is determined using the risk assessment matrix (see Annex 5 to the Methodology). The level of risk is considered lowly significant, when the risk is rated between 1 and 1.5 of total score; moderately significant – when the risk is rated between 1.6 and 2.5 of total score; significant – when the risk is rated between 2.6 and 3.5 of total score, very significant – when the risk is rated between 3.6 and 4 of total score.

CHAPTER IV
DETERMINATION OF RISK MITIGATION MEASURES

17. For the risk with the determined level of risk considered as moderately significant, significant, very significant, mitigation measures shall be prepared and these measures shall be attributed, within the competence, to the responsible authority for setting a deadline for implementing the measure.

18. With regard to the prepared measures for mitigating identified risks, NRA performing entity (service provider) shall prepare a plan for identified risk mitigation measures.

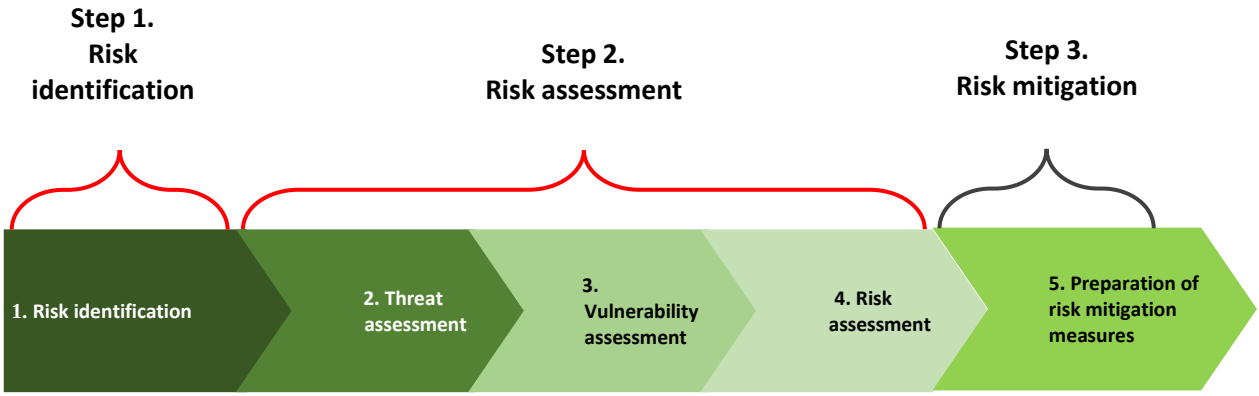
CHAPTER V
FINAL PROVISIONS

19. NRA report shall follow the risk identification, risk assessment and determination of risk mitigation measures describing the undermentioned:
    19.1. Lithuanian economic, geographical, political and legal environment;
    19.2. the functions of institutions in the field of prevention of money laundering and / or terrorist financing;
    19.3. human and financial resources intended for the prevention of money laundering and / or terrorist financing, if this information is available;
    19.4. specific sector, product, service;
    19.5. threat of a sector, product, service and its scoring;
    19.6. vulnerability of a sector, product, service and its scoring;
    19.7. the level of risk of a sector, product, service;
    19.8. risk mitigation measures, if the identified level of risk is considered as moderately significant, significant, very significant.
20. NRA report does not reveal non-public data and information.
21. NRA report in Lithuanian and English shall be published on the website of Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania: www.fntt.lt.
22. Services can be procured for NRA reporting or it may be needed to call upon a private person providing such service.
23. NRA report and Risk Mitigation Plan shall approved by the Working Group to coordinate money laundering and terrorist financing prevention activities, formed by the Order No 154 of the Prime Minister On the Formation of the Working Group as of 2 May 2013.
24. Where this Methodology does not regulate certain NRA performance actions, the methodology of the risks of money laundering and terrorist financing affecting the internal market of the EU approved by the European Commission shall prevail.

_____

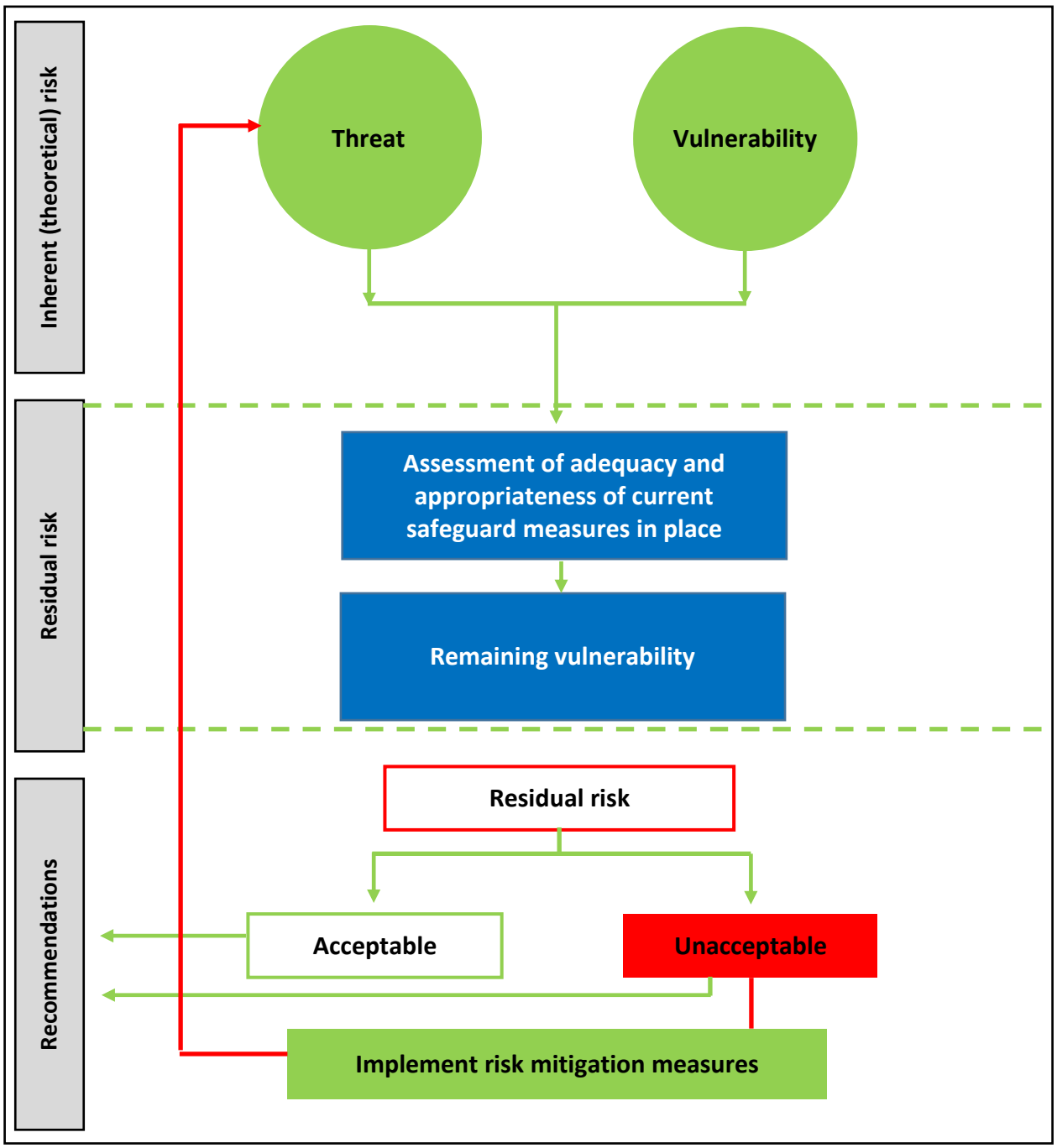
NRA methodology. Annex 1

NATIONAL RISK ASSESSMENT STEPS OF MONEY LAUNDERING AND TERRORIST FINANCING



NRA methodology. Annex 2

FRAMEWORK FOR NATIONAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING



NRA methodology. Annex 3

THREAT ASSESSMENT SCALE

LOWLY SIGNIFICANT (value: 1)	No indicators that criminals have the intention to exploit this modus operandi for ML/TF. The modus operandi is extremely difficult to access and/or may cost more than other options. No indicators that criminals have the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires sophisticated planning, knowledge and/or high technical expertise than other options. The threat related to the use of this modus operandi is lowly significant.
MODERATELY SIGNIFICANT (value: 2)	Criminals may have vague intentions to exploit this modus operandi for ML/TF. The modus operandi is difficult to access and/or may cost more than other options. Few indicators that criminals have some of the necessary capabilities to exploit this modus operandi. The use of this modus operandi requires planning, knowledge and/or technical expertise than other options. The threat related to the use of this modus operandi is moderately significant.
SIGNIFICANT (value: 3)	Criminals have exploited this modus operandi for ML/TF. The modus operandi is accessible and/or represents a financially viable option. The modus operandi is perceived as rather attractive for achieving ML/TF goals. Criminals have the necessary capabilities to exploit this modus operandi. The modus operandi requires moderate levels of planning, knowledge and/or technical expertise. The threat related to the use of this modus operandi is significant.
VERY SIGNIFICANT (value: 4)	Criminals have recurrently exploited this modus operandi for ML/TF. The modus operandi is widely accessible and it implementation is of a relatively low cost. Criminals are known to have the necessary capabilities. The modus operandi requires little planning, knowledge and/or technical expertise required compared to other options. The threat related to the use of this modus operandi is very significant.

NRA methodology. Annex 4

VULNERABILITY ASSESSMENT SCALE

LOWLY SIGNIFICANT (value: 1)	Within the sector/area considered, deterrence measures and controls exist and are effective at deterring money laundering and financing terrorism. **RISK EXPOSURE** • No or very limited products, services that facilitate speedy or anonymous transactions; secured and/or monitored delivery channels; low level of financial transactions; low level of cash based transactions; high quality management of new technologies and/or new payment methods. • Very limited volume of higher risk customers; high ability to manage corporate entities. • No or very limited business and customer based in areas identified as higher risk; • Low level of cross-border movements of funds. **AWARENESS OF THE RISK VULNERABILITY** • Sector concerned shows a satisfactory level of awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). • Competent authorities provide a comprehensive ML/TF risk assessment related to the sector and law enforcement agencies have a high ability to counter ML/TF risks (a range of ML/TF cases is visible and highly likely to be detected, leading to investigation, prosecution and convictions). • Good ability of the financial intelligence unit (hereinafter – FIU) to detect and analyse the risks, to ensure a good functioning of gathering information through suspicious transaction reporting, in particular through the use of tailor-made indicators and a sufficient amount of resources to actually perform the risk-analysis. **LEGAL FRAMEWORK AND CONTROLS** • The existing legal framework is commensurate to the risks inherent to this sector. • Controls defined by the legislation were effectively applied by the sector. Reliable CDD/identification mechanisms are in place. Internal controls are applied by obliged entities in a robust manner (e.g. risk management, record keeping, training). Obliged entities are effectively reporting suspicious transactions to FIUs. • Effective domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a good level of sharing of information.

MODERATELY SIGNIFICANT (value: 2)	Within the sector/area considered, deterrence measures and controls exist and are effective enough at deterring money laundering and financing terrorism. **RISK EXPOSURE** • Limited products, services that facilitate speedy or anonymous transactions; mostly secured and/or monitored delivery channels; rather significant level of financial transactions; rather significant cash based transactions; good management of new technologies and/or new payment methods. • Few higher risk customers; good ability to manage corporate entities. • Some business and customer are based in areas identified as higher risk; • Rather significant level cross-border movements of funds. **AWARENESS OF THE RISK VULNERABILITY** • Sector concerned shows some awareness of the ML/TF risks inherent to its sector (evidence based, actions undertaken, training, allocated resources). • Competent authorities provide a reasonable ML/TF risk assessment related to the sector and law enforcement agencies have a good ability to counter ML/TF risks (a range of ML/TF cases is visible and likely to be detected, leading to investigation, prosecution and convictions). • FIU can detect and analyse the risks, to ensure a good functioning of gathering information through suspicious transaction reporting, in particular using tailor-made indicators. **LEGAL FRAMEWORK AND CONTROLS** • The existing legal framework covers in major parts the risks inherent to this sector. • Most of controls defined by the legislation were applied by the sector. Reliable CDD/identification mechanisms are in place but do not ensure systematically an adequate identification and verification process of a customer. Internal controls are applied by obliged entities to some extent (e.g. risk management, record keeping, training). Obliged entities are reporting few suspicious transactions to FIUs. • Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows a partial sharing of information.
SIGNIFICANT (value: 3)	Within the sector/area considered, deterrence measures and controls have limited effects in deterring money laundering and financing terrorism. **RISK EXPOSURE** • Significant volumes of products, services that facilitate speedy or anonymous transactions; few secured and/or monitored delivery channels; significant level of financial transactions; significant cash based transactions; low management of new technologies and/or new payment methods.

	• Significant volumes of higher risk customers; low ability to manage corporate entities. • Major part of business and customer are based in areas identified as higher risk; • Significant level cross-border movements of funds. **AWARENESS OF THE RISK VULNERABILITY** • Sector concerned shows limited awareness of the ML/TF risks inherent to its sector. • Competent authorities provide for a limited ML/TF risk assessment to the sector and law enforcement agencies have low capacity to counter ML/TF risks (only some ML/TF cases are visible and likely to not be detected). **LEGAL FRAMEWORK AND CONTROLS** • The existing legal framework does not cover the most substantial parts of the risks inherent to this sector. • Controls applied by the sector present significant weaknesses. Ineffective CDD/identification mechanisms are in place. Obliged entities are reporting very few suspicious transactions to FIUs. • Domestic and international cooperation between AML authorities, in particular FIUs and supervisory authorities, allows on few possibilities of sharing of information.
VERY SIGNIFICANT (value: 4)	Within the sector/area considered there are extremely limited or no deterrence measures and controls in place, or they are not working as intended. **RISK EXPOSURE** • Very significant volumes of products, services that facilitate speedy or anonymous transactions; no secured and/or monitored delivery channels; very significant level of financial transactions; very significant cash based transactions; no management of new technologies and/or new payment methods. • Very significant volumes of higher risk customers; ability to manage corporate entities is hardly existent. • Almost all business and customers are based in areas identified as higher risk; • In large part, cross-border movements of funds are prevailing. **AWARENESS OF THE RISK VULNERABILITY** • Sector concerned shows no awareness of the ML/TF risks inherent to its sector. • Competent authorities do not provide for any reasonable ML/TF risk assessment related to the sector and law enforcement agencies have no ability to counter ML/TF risks. **LEGAL FRAMEWORK AND CONTROLS**

	• The existing legal framework does not cover the risks inherent to this sector. • Controls applied by the sector present very significant weaknesses. No reliable CDD/identification mechanisms are in place. Obliged entities are not reporting suspicious transactions to FIUs. • No cooperation between domestic and international AML authorities, in particular FIUs and supervisory authorities.

NRA methodology. Annex 5

RISK ASSESMENT MATRIX

Threat	Very significant (value: 4)	2.2	2.8	3.4	4
	Significant (value: 3)	1.8	2.4	3	3.6
	Moderately significant (value: 2)	1.4	2	2.6	3.2
	Lowly significant (value: 1)	1	1.6	2.2	2.8
		Lowly significant (value: 1)	Moderately significant (value: 2)	Significant (value: 3)	Very significant (value: 4)
		Vulnerability			

Annex 2. Glossary

Anti-money laundering and terrorist financing related acronyms and abbreviations	
Acronym	**Meaning**
AML/CFT	Anti-Money Laundering / Counter-Terrorism Financing
ATM	Automated Teller Machine
BoL	The Bank of Lithuania
CDD	Customer Due Diligence
CIS	The Commonwealth of Independent States
CTR	Currency Transaction Report
DNFBPs	Designated Non-Financial Businesses and Professions
EDD	Enhanced Due Diligence
EU	European Union
FATF	Financial Action Task Force www.fatf-gafi.org
FCIS	The Financial Crime Investigation Service
Fintech	Technology-enabled and technology-supported financial services
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
KYC	Know Your Customer
ML	Money laundering
MO	Modus operandi (Latin: “operating method”), in criminology, distinct pattern or manner of working that comes to be associated with a particular criminal.
MONEYVAL	Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures
MVTS	Money Value Transfer Services
NGO	Non-governmental organization
NPO	Non-for-profit organization
NRA	National risk assessment
OCG	Organized Crime Group
OECD	Organization for Economic Cooperation and Development http://www.oecd.org/
PEP	Politically Exposed Person
SSD	The State Security Department of the Republic of Lithuania
STI	The State Tax Inspectorate
STR	Suspicious transactions reports
TBML	Trade-Based Money Laundering
TF	Terrorist financing
UBO	Ultimate Beneficial Owner