



Národné hodnotenie rizika legalizácie príjmov z trestnej činnosti a financovania terorizmu

**NATIONAL ASSESSMENT OF THE RISK
OF MONEY LAUNDERING AND
TERRORIST FINANCING**



FINAL REPORT

ON THE NATIONAL ASESMENT OF THE RISK

OF MONEY LAUNDERING AND TERRORIST

FINANCING IN THE CONDITIONS OF THE

SLOVAK REPUBLIC

DISCLAIMER

"The National Assessment of the Risk of Money Laundering and Terrorist Financing (hereinafter the "National Risk Assessment") in the Conditions of the Slovak Republic was carried out by self-assessment by the relevant Slovak authorities using the national risk assessment tool developed and on the basis of a contractual relationship with the World Bank. The position and tasks of the World Bank project team were limited to delivering the tool, methodological management, and providing guidance on the technical aspects of the tool and providing a final report on the scope, accuracy and precision of its use. The statistical data and information used to carry out the national risk assessment, as well as findings, final interpretations and opinions based on the national risk assessment, fully reflect the views and position of the relevant Slovak authorities, and in no way reflect the views of the World Bank."

ADDRESS OF THE NATIONAL RISK ASSESSMENT COORDINATOR

Dear colleagues,

Money laundering and the financing of terrorism as a serious anti-social and criminal activity performed in all its forms, and through countless methods, is a serious global problem. At the same time, it is a major challenge in terms of the activities of the competent public authorities as well as of the private sector. Money laundering is a latent threat not only from the point of view of the economy but a real threat to the foundations of a democratic set-up of the country. A special threat is the financing of terrorist activities. Taking into account recent events, it is necessary for these entities to create an efficiently functioning system of legislative, technical and organizational-personnel countermeasures, while emphasizing the activity of selected entities at the national level in the fight against this phenomenon.

For this reason, the Slovak Republic, as a democratic and legal state that is a valid member of the international community, moved towards the implementation of the national assessment of the risk of money laundering and terrorist financing in accordance with accepted international standards. In the conditions of the Slovak Republic this is the first and rare project implemented to this extent and in the mentioned area. Its uniqueness lies above all in the horizontal nature of the area under review and in the way in which it was approached. In addition to the results, the process of national risk assessment itself has already brought an extraordinary added value. The self-evaluation method is a challenge for each of us, whether in the personal or working sphere of our lives.

Notwithstanding the fact that the process of the assessment was a thorny path in some moments, I am honoured to present to you the results of the maximum effort and above all the personal deployment of all members of the group of public and private sectors composed of nearly 70 members. An important element of the whole system was the involvement of World Bank officials. Their contribution was indeed invaluable with regard to internal assessment processes.

The National Risk Assessment Report presents a comprehensive picture of the threats and vulnerabilities of the national system, with the greatest attention being paid to the elements that negatively affect the overall level of ML and TF risk. At the same time, it demonstrates a high level of professionalism and self-reflection of the stakeholders.

The National Risk Assessment Report is not a police assessment and definitely not just a document for the needs of the police. It is addressed to a wide range of addressees, ranging from intelligence services, law enforcement bodies, courts, supervisory bodies to policy-makers. It focuses significantly on the powers of the private sector and thus covers the issues of citizens' ordinary lives. The presented version is a consolidated version of the assessment. The detailed assessment consistently reflecting all the elements of the World Bank methodology is available to sector experts and private sector representatives. It should also be noted this report is not a one-time document. It is a continuous process. The development of sectoral policies under the Action Plan should result in an increase in the efficiency of the whole system. The natural consequence is its regular updating.

In conclusion, please allow me to express my sincere thanks to all involved employees of the relevant state authorities and the institutions and the representatives of the private sector for their work and their personal contribution to the national risk assessment process. However, I would especially like to thank my predecessor and members of the Financial Intelligence Unit of the National Criminal Agency, the Presidium of the Police Force, who, despite their unfavourable personal and organizational situation, performed decisive coordination tasks within this challenging project.

Pavol Vorobjov
Coordinator
National Assessment of the Risk
of Money Laundering and Terrorist Financing

TABLE OF ACRONYMS

AML/CTF – Anti-Money Laundering/Countering the Financing of Terrorism (Combating the financing of terrorism)
AMO – Asset Management Office
CDD – Customer Due Diligence
EEC – European Economic Community
EU – European Union
FATF – Financial Action Group
FD SR – Financial Directorate of the Slovak Republic
FA SR – Financial Administration of the Slovak Republic
FSJ – Financial Intelligence Unit of the National Criminal Agency of the Presidium of Police Force
GPO SR – General Prosecutor's Office of the Slovak Republic
GDP – Gross Domestic Product
RD PF – Regional Directorate of the Police Force
FACO – Financial Administration Criminal Office
BO – beneficial owner
KYC – „Know Your Customer“
MEKO – Interdepartmental Expert Coordination Body on Combating Crime
MF SR – Ministry of Finance of the Slovak Republic
MISO (LP) – Multidisciplinary Integrated Group of Experts to Eliminate ML and TF
ML/TF – money laundering and terrorist financing
MoD SR – Ministry of Defence of the Slovak Republic
MoJ SR – Ministry of Justice of the Slovak Republic
Moi SR – Ministry of Interior of the Slovak Republic
NBS – National Bank of Slovakia
NRA – National Assessment of the Risk of Money Laundering and Terrorist Financing
OECD – Organisation for Economic Co-operation and Development
AF SR – Armed Forces of the Slovak Republic
DD PF – District Directorate of the Police Force
P PF – Presidium of the Police Force
SIS – Slovak Information Service
SR – Slovak Republic
SPO GPO SR - Special Prosecutor's Office (USP) of the General Prosecutor's Office of the Slovak Republic
VS – Military Intelligence
V4 – An alliance of the so-called Visegrád Group countries (Visegrád Four): Czech Republic, Poland, Hungary, Slovak Republic
WBG – World Bank Group

EXECUTIVE SUMMARY.....	9
INTRODUCTION	22
PART 1 – RISK OF LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY	28
CONTEXTUAL FACTORS OF THE SLOVAK REPUBLIC IN RELATION TO LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY.....	28
1.1. THREAT OF LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY AT NATIONAL LEVEL.....	31
1.1.1. GENERAL ASSESSMENT OF THE THREAT OF LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY	31
1.1.2. ASSESSMENT OF THE BASIC SOURCE ML THREATS ARISING FROM THE SPECIFIC TYPES OF CRIMINALITY AND THE RELATED FORMS OF CRIMINAL ACTS	41
CRIMINAL OFFENSES AGAINST PROPERTY	43
CRIMINAL OFFENSES OF ECONOMIC NATURE	44
PARTIAL TYPES OF CRIME	45
CRIMINAL VIOLENCE.....	48
MORAL CRIME	49
1.1.3. ASSESSMENT OF THREATS ON THE BASIS OF LEVELS AND QUALITY OF DETECTION, INVESTIGATION AND CRIMINAL PROSECUTION OF THE CASES OF LEGALIZATION OF PROCEEDS OF CRIME	50
ANALYSIS OF THE CASES OF LEGALIZATION OF PROCEEDS OF CRIME.....	50
IDENTIFICATION OF PROCEEDS AND WITHDRAWAL OF PROCEEDS	54
ML GEOGRAPHICAL FACTORS	56
RELATED PREDICATE CRIMINAL OFFENCES:.....	57
1.2. VULNERABILITY WITH RESPECT TO THE LEGALIZATION OF PROCEEDS OF CRIME AT NATIONAL LEVEL	61
1.2.1 COUNTRY’S ABILITY TO FIGHT AGAINST THE LEGALIZATION OF PROCEEDS OF CRIME.....	61
QUALITY OF AML POLICY AND STRATEGY	62
EFFECTIVENESS OF THE DEFINITION OF THE OFFENSE OF LEGALIZATION OF PROCEEDS OF CRIME	63
EFFECTIVENESS OF CROSS-BORDER CASH CONTROLS	64
QUALITY OF FINANCIAL CRIME DETECTION	65
QUALITY OF CRIMINAL PROSECUTION OF FINANCIAL CRIME.....	80
QUALITY OF COURT JUDGMENTS.....	85
QUALITY OF A FRAMEWORK FOR SEIZURE OF PROPERTY AND WITHDRAWAL OF PROCEEDS OF CRIME	88
ASSESSMENT OF VULNERABILITY IN CONNECTION WITH CORPORATIONS ACTIVITIES	92
DETERMINATION OF PRIORITIES BASED ON NATIONAL VULNERABILITY ASSESSMENT	94

1.2.2 GENERAL EVALUATION OF THE OVERALL LEVEL OF VULNERABILITY OF THE SECTORS OF NATIONAL ECONOMY.....	95
PART 2 – ASSESSMENT OF THE VULNERABILITY OF LEGALIZATION OF PROCEEDS OF CRIME IN PARTICULAR SECTORS OF THE NATIONAL ECONOMY	99
2.1. BANKING SECTOR	99
PROVISION OF FINANCIAL INCLUSION PRODUCTS.....	118
2.2. SECTOR OF NON-FINANCIAL BUSINESSES AND PROFESSIONS.....	120
2.3. OTHER FINANCIAL INSTITUTIONS SECTOR	154
2.4. INSURANCE SECTOR	176
3.1. THREAT OF TERRORISM IN THE CONDITIONS OF THE SLOVAK REPUBLIC	200
NATIONAL SOURCES OF TERRORIST THREAT	200
REGIONAL SOURCES OF TERRORIST THREATS	201
GLOBAL SOURCES OF TERRORIST THREATS	202
TRANSIT AS THE SOURCE OF TERRORIST THREAT.....	202
3.2. ASSESSMENT OF THE RISK OF TERRORIST FINANCING	204
3.2.1. THREAT OF TERRORIST FINANCING.....	204
DETECTION AND VERIFICATION OF TERRORIST FINANCING	204
CASH TRANSIT CONTROL.....	207
THREAT OF MISUSE OF VIRTUAL CURRENCIES FOR TERRORIST FINANCING	208
UNIDENTIFIED FUNDS POTENTIALLY INTENDED FOR TERRORIST FINANCING	209
3.2.2. VULNERABILITY OF TERRORIST FINANCING	210
QUALITY OF LEGISLATION	210
QUALITY OF INTELLIGENCE INFORMATION.....	214
EFFICIENCY OF THE SYSTEM OF REPORTING UNUSUAL TRANSACTIONS RELATED TO THE TERRORIST FINANCING, MONITORING AND ANALYSIS	215
ADEQUACY OF RESOURCES	216
EFFICIENCY OF INTERNATIONAL COOPERATION.....	216
AWARENESS AND INVOLVEMENT IN FIGHT AGAINST TERRORIST FINANCING	218
GEOGRAPHIC AND DEMOGRAPHIC FACTORS	219
OTHER FACTORS	220

EXECUTIVE SUMMARY

The Slovak Republic is a landlocked country situated in the geographical centre of Europe. It is bordered directly by five countries - Austria, the Czech Republic, Poland, Ukraine and Hungary. Due to its geographical location, size and population, it can be classified as a smaller country, with little or no impact on the global economy, international, political situation and global financial systems¹. The Slovak Republic has a standard system of government, a relatively steady political situation, applies the principles of a democratic state and a positive approach to the rights of the minority population by the individual branches of public administration. Despite the sustained and dynamic growth of significant macroeconomic indicators, the Slovak Republic cannot be classified as the financial centre of Central Europe or as a country that would allow to reduce the tax burden on domestic and foreign business entities.

The positive economic developments and increasing the country's "wealth" should also be reflected in the activities of authorities dealing with the detection and verification of entities that can use it in their favour by committing serious anti-social (and also illegal) activities.

Overall **LEVEL of the RISK** of legalization of proceeds of criminal activity
is at the **MEDIUM LEVEL**.

Overall level of **THREATS** is **MEDIUM**
Overall level of **VULNERABILITY** is **MEDIUM**

ML THREATS

The overall level of the ML threats in SR conditions is **medium** with an increasing trend. The extent of unrecorded proceeds of criminal activity not sanctioned by criminal prosecution is substantially higher.

Geographical factors affecting the overall level of threat:

- National ML threat: **“high”**
- Foreign ML threat: **“medium high”**
- Unidentified origin of ML threat: **medium high**

However, for the purposes of proper assessing the ML/TF risk in SR conditions, it is necessary to understand not only the overall context of the long-term development of crime, but it is necessary to consider its impact and factors affecting the extent and volume of proceeds coming from crime, but also a number of other factors that may (and have) the impact on crime. In the context of ML and TF risks, it is mainly the perpetrator's motive in the form of proceeds, the possibilities of the SR for their placement, and also, for example, the ratio of reported and unreported crime. In the long term, the Slovak Republic takes

¹Please add: Area: 49,035 km², Borders 1,652.6 km with HU, Czech R., PL, UA and AT. Population: 5 429 000, GDP: 85 bil. EUR Average pay in 2017 of 954 EUR, minimum pay in national economy in 2017 amounting to 435 EUR, unemployment in 2017 at 8.1%,

countermeasures against the persistent threats arising from the existing grey and black economy and adopts appropriate legislative and institutional measures aimed at effectively combating and suppressing such illegal activity and in particular its accompanying phenomena such as the legalization of proceeds of criminal activity or the financing of terrorism. A wider process includes extraordinary extensive measures in the field of tax collection, combating tax evasion and tax crime. The development of the security situation on the territory of the Slovak Republic in terms of the number of detected crimes can be considered as extremely positive. In recent years, there has been a significant decline in the overall incidence of criminal acts. In the period under review, the overall incidence of criminal acts dropped by about 21%.

Based on the overall context of long-term crime development and the determination of the potential of the type of crime and individual predicate offenses as the source area of crime proceeds generation, the following estimated unrecorded proceeds and the following GENERAL ML THREATS AND RELATED TRENDS have been set:

- o **Criminal offenses against property (theft) – 38%,**
Estimated amount of unrecorded proceeds - the ratio of unrecorded proceeds is slightly higher
Threat level – medium
Trend – falling
- o **Criminal offenses of economic nature (tax crimes, fraud, damage to the financial interests of the European Communities) – 17.51%,**
Estimated amount of unrecorded proceeds - the ratio of unrecorded proceeds is (disproportionately) higher
Threat level – medium
Trend - no change
- o **Specific partial types of crime (corruption, drug-related crime, organized form of committing crime, cybercrime) – 2.61%,**
 - Organized crime**
Estimated amount of unrecorded proceeds - the ratio of unrecorded proceeds is substantially higher
Threat level – high
Trend - no change
 - Cybercrime / computer crime in a broader sense**
Estimated amount of unrecorded proceeds - the ratio of unrecorded proceeds is substantially higher
Threat level – high
Trend - increasing
 - Drug-related crime**
Estimated amount of unrecorded proceeds - the ratio of unrecorded proceeds is substantially higher
Threat level – medium
Trend – increasing
 - Corruption (in a broader sense)**

Estimated amount of unrecorded proceeds: - the ratio of unrecorded proceeds is higher

Threat level – medium

Trend – no change

- o **Criminal violence** (illegal production, possession and trading in guns, ammunition and explosives, racketeering, robbery) – **2.12%**, and

Estimated amount of unrecorded proceeds - except for carrying concealed weapons and arms trafficking, where the ratio of unrecorded proceeds is substantially higher, the ratio of unrecorded proceeds for criminal violence is not significant

Threat level – medium

Trend – falling

- o **Moral crime** (human trafficking, procuring and soliciting prostitution, prostitution, child pornography) – **0.13%**.

Estimated amount of unrecorded proceeds – except for human trafficking, where the ratio of unrecorded proceeds is substantially higher, the ratio of unrecorded proceeds for moral crime is not significant

Threat level – medium

Trend – increasing

Based on the evaluation of all ML cases prosecuted in the Slovak Republic in the period under review, the following predicate offenses were identified :

- a) **Theft – 71.93%** (mainly theft of motor vehicles or motorcycles, theft of a thing and theft by breaking and entering),
- b) **Fraud – 17.42 %** (mainly the cases of unauthorized transfer of funds for products and services
- c) **Other predicate offenses – 5.92%** (robbery, carrying concealed weapons and arms trafficking, tax and insurance evasion, failure to pay tax and insurance, abuse of public authority powers, criminal conspiracy, illicit manufacture of narcotic drugs and psychotropic substances, poisons or precursors, and trafficking in them,
- d) **Counterfeiting identification data of a motor vehicle – 4.98%**.

In the SR, there are no reliable statistical data that would quantify the value of the proceeds of crime with a sufficient level of explanatory power. However, the SR has systematically obtained data on the amount of damage caused. Under SR conditions, the amount of damage is an important qualification factor determining the seriousness of the offense. In principle, however, it can be stated that the amount of the reported damage is higher than the potential volume of proceeds of criminal activity.

Overview of criminal offences generating the highest damage:

- a) Fraud
- b) Credit fraud,
- c) Theft,
- d) Embezzlement,
- e) Tax and insurance evasion,

- f) Tax fraud, and
- g) Failure to pay tax and insurance.

By thoroughly analysing the practices and activities that ML perpetrators actively used to hide the illegal origin of generated income and proceeds, the Working Group identified the most used forms and methods of legalization:

- More than half of the proceeds of criminal activity are subject to immediate consumption by the perpetrator of the predicate offense, without specific elements of the legalization moment,
- Transfers to accounts at banks and branches of foreign banks and subsequent withdrawals from these accounts,
- Sale of stolen and modified things to cover the origin from the crime.

No sophisticated forms of legalization have been identified, e.g. using placement of proceeds abroad or by engaging professional individuals.

Geographical factors for ML

1,113 Slovaks were involved in ML cases, representing a 95.54% share of the total number of ML cases (1,165 cases); and foreigners were involved in 53 cases of 99 cases (an 8.50% share). It is clear from the analysis that statistically the proceeds generated in the Slovak Republic still prevail.

In an overwhelming majority of ML cases, the SR was the target country (in 1,059 ML cases, representing a 90,90% share). Other target countries: Ukraine, Poland and Hungary.

With respect to the country of origin, the SR had the highest representation (63.52%) in ML cases. Other countries of origin: Germany, Austria, Czech Republic, Italy.

In the period under review, ML cases with the involvement of so-called off-shore countries or tax havens, were not prosecuted.

ML VULNERABILITY

The overall level of the ML threat in SR conditions is moderately high

Factors affecting overall vulnerability:

- Ability of the country to fight against ML - moderate
- Overall vulnerability of the national economy sectors – medium-high

The result of the country's overall ML vulnerability at national level points to the fact that the level of measures in the fight against money laundering is average and a more **problematic area is mainly the low effectiveness of these measures**. The reason for the weaker ability of the country to fight against legalization is a poor quality of searching, detection of criminal activity, the quality of prosecution, the quality of judgments and the

deterioration in the quality of the framework for the seizure and ultimate confiscation of illegally acquired property.

The resulting average level of overall sectoral ML vulnerability is primarily determined by the **medium-high vulnerability** of the banking sector, which is the most important sectors from among sectors under review for the national economy and the financial sector of the country. The medium-high vulnerability has been assessed for financial agents and financial advisers, legal entities and natural persons authorized to provide organizational and economic consulting, gambling operators and management companies.

A) Ability of the country to fight against ML

Significant determinants of the low level of effectiveness of law enforcement authorities in detecting financial crime are:

- Insufficient staffing and financial resources of the FSJ, which has a direct and adverse impact on performance of its core activity. These shortcomings result mainly from the organizational status of the FSJ in the structure of the PF SR. Also, the absence of a clear concept of job performance, which is obviously due to the fluctuation of managers, also has a negative impact.
- In the Slovak Republic there is no specialization in the field of detection of the legalization of proceeds of criminal activity, especially in the absence of specialized departments dealing with the so-called financial investigation. This fact also results in insufficient seizure and confiscation of proceeds and income of criminal activity (and the compensation for property damage or economic damage). This shortcoming is clearly horizontal in nature and directly covers the criminal prosecution of financial crime.
- Absence of a central bank account register and the impossibility of tracking online account transactions.
- Absence of systematic preparation of law enforcement authorities, including courts in the area of money laundering and property seizure
- Absence of efficient information systems for managing files and documents and then obtaining relevant statistical data. From the point of view of the horizontal approach to effective verification and detection of crime, the negative fact is also the absence of interconnection between current police, prosecution and court systems
- In the context of property seizure, the problem is also the missing entity, which would manage all the seized assets (and the execution of property-related decisions) in a comprehensive manner. Several competent authorities point to the absence of the Office for the Administration of Seized Proceeds and Things from Criminal Activity and the Office for the Return of Seized Proceeds and Things from Criminal Activity to authorized owners and injured (AMO)

- Application problems have been identified, in particular, in the area of the seizure of assets acquired for proceeds coming from criminal activity obtained by another person, as well as for certain conditions for the use of seizure concepts available to ensure the execution of property punishment, e.g., demonstrating a reasonable concern that the execution of this punishment will be impaired or difficult. The seizure of a substitute value also appeared problematic. Practically it was difficult to seize the assets of third parties. It was not possible to seize third-party assets, except for the property of the perpetrator which was mixed with the third party's property. Operational police officers in fact had no means of seizing the proceeds of crime under the Act on Police Force. The legislation did not allow sufficient seizure of a thing and property on the grounds that in some cases it was linked to the accused person's procedural position.

B) Overall vulnerability of the sectors of the national economy: the "medium-high" level

Based on the generalization of the results of the evaluation, it is possible to identify the following **common factors within procedural vulnerability**, which significantly affect the vulnerability in several sectors under review:

- Insufficient awareness of obliged entities of the ML/TF risks and their management,
- Non-compliance with otherwise adequate legislation,
- Insufficient number of inspections carried out with obliged entities and property associations carried out by AML/CTF regulators,
- Insufficient methodical and training activities by regulators.

BANKING SECTOR

Overall identified level of vulnerability of the sector: **medium-high level of vulnerability**

Procedural vulnerability

The assessment of the procedural aspect related to the performance of the activities and internal processes of the individual entities of the banking sector as well as the supervisory and control authorities has identified the following vulnerabilities:

- Effectiveness of supervisory practices and methods
- Existence and enforcement of administrative sanctions
- Existence and enforcement of criminal sanctions,
- Knowledge of bank employees about AML measures,
- Effectiveness of the bank responsible for compliance,
- Effectiveness of UTR monitoring and reporting,
- Availability and access to beneficial ownership information,
- Availability of independent information sources.

Of the 15 most frequently used products and services within the Slovak banking market, the following products were evaluated as the most vulnerable in terms of ML:

a) Payment accounts of legal entities - small and medium-sized enterprises - high level of vulnerability

Determinants of vulnerability:

- Amount of funds deposited and the high level of cash operations,
- Funds deposited may relate to tax crime,
- Transactions by small and medium-sized enterprises are considered to be most often related to carousel fraud and unauthorized excessive VAT deductions,
- Defects in the taking of CDD measures (including KYC) by obliged entities, and determination of client risk,
- Frequent cross-border transactions into risk countries or countries marked as tax havens or offshore countries,

b) Payment accounts of legal entities – large business entities - medium-high level of vulnerability

Determinants of vulnerability:

- Amount of funds deposited,
- Funds deposited may relate to tax crime,
- Transactions by large business entities are considered to be most often related to carousel fraud and unauthorized excessive VAT deductions,
- Defects in the taking of CDD measures (including KYC) by obliged entities, and determination of client risk,
- Frequent cross-border transactions into risk countries or countries marked as tax havens or offshore countries,

c) Private banking service – high level of vulnerability

Determinants of vulnerability:

- Defects in the taking of CDD measures (including KYC) by obliged entities, and determination of client risk with respect to his social position and social influence and links to politically active persons with decision-making powers as well as at the central and regional levels,
- Absence of the duty to report by banks and branches of foreign banks.

FINANCIAL INCLUSION PRODUCTS

With respect to the total amount of basic banking products, their internal characteristics and the measures taken by banks and branches of foreign banks, it can be noted that the level of vulnerability of financial inclusion products in Slovak conditions is at a low (very low) level.

SECTOR OF NON-FINANCIAL ENTITIES

Overall identified level of vulnerability of the sector: **moderate level of vulnerability**

The assessment of the procedural aspect related to the performance of the activities and internal processes of the individual entities of the non-financial sector as well as the supervisory and control authorities has identified the following vulnerabilities:

- Insufficient knowledge of the AML/CTF area and staff training,

- Deficiencies in customer due diligence and in determining the origin of the client's funds,
- Inefficiency of supervision,
- Demonstrating the integrity of the staff,
- Inefficient recognition and monitoring of UTRs,
- Inefficient initial control mechanisms when issuing a license, or when registering,
- Availability and enforcement of criminal and administrative sanctions,
- Possibility of setting up an unlimited number of companies,
- Carrying out activities without transparent trade,
- Non-performance of internal controls,
- Failure to keep written documents,
- Non-use of the possibility of information exchange according to the AML/CTF Act,
- Use of cash payment operations,
- Inefficiency of compliance of functions,
- Absence of independent information sources,
- Lack of the awareness of the risks of the profession, and
- Absence of financial beneficiaries register.

An overview of entities operating in the non-financial sector identified as entities with the highest level of ML vulnerability.

a) A provider of asset or service management for commercial companies – medium-high level of vulnerability

Determinants of vulnerability

- The said sphere of business (providing asset management services or services for commercial companies) is not recognized by the Trade Licensing Act. These actions are performed under the following authorizations for:
 - Property rental associated with the provision of other than basic services related to rental,
 - Organizational and economic consultancy,
 - Bookkeeping or administrative services,
- Knowledge and awareness of AML/CTF,
- Effectiveness of AML/CTF controls,
- Integrity of the staff,
- Issue of business licenses,
- Recognition and monitoring of UTRs,
- Availability and enforceability of sanctions,
- Possibility of setting up an unlimited number of companies which are subsequently provided free of charge to other owners who subsequently provide the services at the price at which the change of the owner is compensated,
- Non-transparent performance of the activity (without proper trade license).

b) Accountant – medium-high level of vulnerability

Determinants of vulnerability

- Conditions for the issue of free trade,
- Possibility of setting up an unlimited number of companies, in the case of withdrawal of licence to pursue business in one company, a natural person or a legal person may

continue to provide this activity through another company with the same sphere of business matter,

- Effectiveness of AML/CTF controls,
- Awareness and knowledge of AML/CTF areas and ML/TF risks associated with the sphere of business,
- Non-performance of internal control,
- Limited possibilities to ensure flow of information on AML/CTF,
- No use of the possibility of exchanging information between obliged entities according to the relevant provisions of AML/CTF Act,
- Failure to keep written documents on transactions according to the relevant provisions of AML/CTF Act.

SECTOR OF OTHER FINANCIAL INSTITUTIONS

Overall identified level of vulnerability of the sector – border between the medium-low and medium level

The assessment of the procedural aspect related to the performance of the activities and internal processes of the individual entities of the non-financial sector as well as the supervisory and control authorities has identified the following vulnerabilities:

- Average knowledge of the laws, principles and procedures for combating ML/TF by both employees and the obliged entity,
- Absence of awareness of the fact that the OFIs are the obliged entities and the resulting obligations,
- Unclear number of entities actually active in the OFI sector,
- Absence of powers for the performance of AML/CTF supervision for NBS staff performing foreign exchange supervision,
- Absence methodological guidance for performance of ML/TF prevention obligations for individual OFI categories,
- Absence of joint inspections of the FSJ and the NBS in order to develop mutual cooperation and exchange of experience,
- Low number of FSJ employees and the low number of controls performed in proportion to the number of obliged entities in OFI sector, and
- Absence remote controls, despite legal authorization to do so.

An overview of entities operating in the non-financial sector identified as entities with the highest level of ML vulnerability.

a) Financial agent and financial advisor - medium level of vulnerability

Determinants of vulnerability:

The level of vulnerability is adversely affected by the high number of obliged entities, an activity based exclusively on the mediation of the products of other institutions.

b) Financial leasing or other financial activities according to a special regulation - medium level of vulnerability

Determinants of vulnerability:

The level of vulnerability is adversely affected by the ability to make cash payments and a high number of obliged entities.

c) Payment institution, payment service agent, electronic money institution - medium level of vulnerability

Determinants of vulnerability:

The level of vulnerability is adversely affected by the ability to make cash payments and use products without the physical presence of a client.

INSURANCE SECTOR

Overall identified level of vulnerability of the sector - **medium level of vulnerability**

The assessment of the procedural aspect related to the performance of the activities and internal processes of the individual entities of the insurance sector as well as the supervisory and control authorities has identified the following vulnerabilities:

- Absence of adequate measures to verify BO identification,
- Absence of risk-oriented approach and inclusion of clients in risk groups,
- Absence of a list of offshore countries
- Absence of controls for performance of AML duties,
- Insufficient consideration of risks arising from ML and FT,
- Inconsistent implementation of CDD,
- Non-detection of the origin of funds on entry into the system,
- UTR reporting is oriented to the exit of funds from the insurance segment (redemption, termination of insurance),
- Shops or the client contained in the UTR report is not then passed into the higher risk category,
- Only formal knowledge of staff on AML, which results mainly in serious deficiencies in practical application on specific cases,
- Low quality of the assessment and reporting of UTRs, as well as business transaction assessment records.

SECURITIES SECTOR

Overall identified level of vulnerability of the sector – **medium-low level of vulnerability**

The assessment of the procedural aspect related to the performance of the activities and internal processes of the individual entities of the securities sector as well as the supervisory and control authorities has identified the following vulnerabilities:

- Insufficient application of legislation,
- Ineffective application of preventive AML/CTF measures,
- Insufficient knowledge and awareness of ML/TF risks and their management,
- Non-standard transactions with financial instruments and transaction monitoring,
- Low number of controls performed by FSJ,
- Non-imposition of sufficiently dissuasive sanctions,

- Low level of cooperation between regulators and professional organizations and obliged entities,
- Absence of a central financial beneficiaries register,
- Absence of a central bank account register.

An overview of entities operating in the non-financial sector identified in the assessment as entities with the highest level of ML vulnerability.

Management companies - medium level of vulnerability

Transactions executed on behalf of another person, non-transparent follow-up transactions, transfers of securities between entities from different countries, receiving funds from clients from risk countries (especially tax havens and offshore countries) or from sanctioned countries, may have an adverse impact on the level of risk. Also, clients with unclear ownership structure, sophisticated schemes, and clients with a high volume of funds the source of which may be problematic from the point of view of AML/CTF, also pose a risk.

TERRORIST FINANCING RISK

Overall **LEVEL** of the **RISK** of terrorist financing
is at the **MEDIUM-LOW LEVEL**.

Overall level of **THREATS** is **LOW**
Overall level of **VULNERABILITY** is **MEDIUM-LOW**

THREAT OF TERRORIST FINANCING

The overall level of the TF threats in SR conditions has been identified as low. In the assessment, it was necessary to take into account in particular the overall current threat of terrorism in relation to the SR and the ability of all entities involved in the prevention, detection, investigation and prosecution of TF cases.

Due to its geographical location, size and population, the SR can be classified as a smaller country, with moderate or low impact on the world economy, international political situation and global financial systems. A relatively steady political situation, standard state-legal establishment and the application of the principles of a democratic state, without any reported attempts for a violent change in the political condition, a positive approach to the rights of minorities by individual public administration bodies does not create conditions for the occurrence or the formation of groups of the population that would promote or enforce their claims in a particularly radical or violent manner (e.g., related to fundamental changes in the functioning of the state).

Based on the results of the relevant authorities in the field of acquiring and evaluating knowledge and information on potential or potential security threats to the Slovak Republic and its citizens on the territory of the SR, it can be assessed that the overall threat of a terrorist attack by domestic actors was assessed as "low" in the period under review.

By generalizing the information resulting from the UTR reports received, it can be concluded that transactions and business relationships are monitored consistently from FT's point of view. Transactions of entities that might be related to countries posing the risk of Islamist and non-Islamist terrorism, are investigated with particular emphasis. The EU and UN sanctioning regimes are consistently respected.

The threat of cross-border cash transfers for TF purposes is low with respect to individual determinants related to the activity of customs authorities, cooperation between competent authorities, the geographical location of the SR and others, in particular logistical conditions.

In the period under review, no case of terrorist financing in connection with the SR was reported in the Slovak Republic, i.e. there was no prosecution by the Slovak law enforcement authorities regarding TF. Even in the context of the investigation of suspected cases of terrorism, the elements of its financing in harmony with the requirements of the FATF standards have not been confirmed. There was also no case of abuse of the humanitarian or charitable activities of non-profit organizations operating on the territory of the Slovak Republic for the purposes of TF or other use (misuse) of funds obtained through public collections.

TERRORIST FINANCING VULNERABILITY

The overall level of TF vulnerability in Slovak conditions was identified at a **medium-low** level. The following determinants and vulnerability factors directly affected the overall level:

- a) The quality of the legal framework governing the status and activities of the competent authorities and the circumstances having direct or indirect effect on TF elimination – medium-low impact on vulnerability,
- b) The quality of intelligence information and its use - medium-low impact on vulnerability,
- c) Effectiveness of the UTR reporting system, monitoring and analysis - medium-low impact on vulnerability,
- d) Adequacy of sources - medium-low impact on vulnerability,
- e) Effectiveness of international cooperation - low level of impact on vulnerability,
- f) Awareness and involvement in the fight against TF - low level of impact on vulnerability,
- g) Geographic factors and demographic factors - medium-low impact on vulnerability,

h) Other factors:

- Non-investment pooled asset funds – medium-low impact on vulnerability,
- Exchange activity – low level of impact on vulnerability,
- Financial inclusion products – low level of impact on vulnerability.

INTRODUCTION

Objectives of the national assessment of the risk of legalization of proceeds of criminal activity and terrorist financing

The national assessment of the risk of legalization of proceeds of criminal activity and terrorist financing was the very first assessment of this type in the Slovak conditions. It should significantly help the relevant authorities in identifying and evaluating internal and external threats that affect, to a greater or lesser extent, their everyday activities and their roles in the fight against this antisocial activity. This purpose is attained by detailed analysing individual types of predicate offenses, in particular as regards the origin and direction of funds, the use of a particular sector (product or service) for the purpose of concealing the origin of funds or making it impossible to obtain further information from law enforcement authorities. It also provides a clear view of weaknesses and gaps in the national AML and CTF system, including preventive, prophylactic and repressive measures. It is precisely the identification of the most vulnerabilities that will allow setting the priorities in order to make the national AML/CTF system more effective.

An important part of the NRA is assessing the vulnerability of products and services provided by financial and non-financial sector representatives. As a result, the SR should be able to determine which areas of the private sector are most frequently used to place, stratify and integrate income and proceeds generated from criminal activity, and what methods or channels are most often used to finance terrorism. The comparison of the individual categories of obliged entities operating within a single sector as well as comparisons of mutual sector's vulnerability was equally important. The results obtained should enable, in particular, control and supervisory bodies to develop targeted AML/CTF controls for high-risk products and services.

Each NRA includes a risk assessment for financial inclusion products². In this respect, the SR was not an exception and assessed the ML and TF risks resulting from the core banking product in order to prepare measures appropriate to the identified risk.

The NRA results and findings must also be used in the adoption of managerial decisions with a view to maintaining proportionality in the allocation of personnel and other resources, i.e. the application of the so-called "risk-oriented approach".

The process of national assessment of the risk of legalization of proceeds of crime and the financing of terrorism

MISO-LP established within MEKO recommended the Ministry of Interior representatives to contact World Bank representatives in the matter of cooperation in the implementation of NRA. This institution is the global leader in providing consulting services in connection

² Financial inclusion is the process of securing access for low-income and otherwise disadvantaged sections of the population to financial services in a reasonable time, at an affordable price and in a reasonable quality. In addition to this clearly social level, there is another level that will allow this section of the population to move into a formal financial system. Part of this process must also necessarily be increased financial literacy and financial discipline. Under the conditions of the Slovak Republic, it is the so-called "basic banking product".

with NRA implementation. At present, it provides advice in approximately 80 countries of the world, regardless of whether they are major financial centres, developing countries or traditional developed countries.

The NRA process is a set of stages logically following one upon the other, each of which has its own rules and peculiarities. None of them can be omitted. The whole process therefore required a proactive approach of all participants and, of course, their commitment to face the challenges that accompanied the process.

The first meeting of the NRA Working Group took place in October 2015. The relevant working group composed of the representatives of all relevant departments of P PF, GPO SR, MoF SR including FA SR, MoJ SR, NBS, SIS and MoD SR. An integral part of the Working Group were representatives of the private sector, in particular representatives of professional associations and chambers. The key for the participation of individual departments or organizational units was their participation in the national AML/CTF system at any level and area. The representatives of the Academy of the Police Force in Bratislava had a special position in the Working Group, who integrated the knowledge and input of the academic or scientific circle in the field of ML and TF at scientific level. Their research into the grey and black economy represented an added value for the NRA process. The said public authorities and institutions appointed a total of 65 experts who actively and intensively dealt with a whole range of tasks and responsibilities arising from individual NRA processes. It should also be noted that the representatives of the entities set up their own sectoral structures to support the sectoral outputs for that purpose. An essential element in the process of NRA was its overall coordination and management. With regard to the methodology and internal logic of the evaluation mechanism, the members of the NRA working group (with regard to job classification and expert focus) were divided into eight teams responsible for evaluating the relevant areas. Three teams had a general focus – a team for the assessment of ML threats at national level, a team for the assessment of ML vulnerability at national level, and a team for the assessment of TF risk at national level. The role of the remaining five teams was to evaluate individual sectors of the national economy, namely the banking sector, the securities sector, the insurance sector, the financial institutions sector and the non-financial sector, including the free legal professions. The ML risk assessment in relation to financial inclusion products was carried out within the framework of the banking sector assessment, given the close linkage and preliminary information on the condition of financial inclusion in the Slovak Republic. The FSJ was entrusted with the coordination of the whole NRA process and activities of individual teams with respect to the position of the central national unit in the field of preventing and detecting ML and FT, as its position is defined by law³.

The essence of each NRA, irrespective of the fact whether the evaluated country uses an external entity service to perform it, has been collecting and gathering sufficient relevant qualitative and quantitative data for a predetermined period. Having examined the legislative and institutional developments in the AML/CTF area in the Slovak Republic and taking into account the current externalities affecting this development, the NRA Working Group decided to evaluate the 2011-2015 period. The, the activity of individual teams was also adapted to the fact. The ways and methods for collecting relevant information,

³ Act No. 297/2008 Coll. on the Prevention of Legalization of Proceeds of Criminal Activity and Terrorist Financing and on Amendments and Supplements to Certain Acts as amended by the further acts.

statistical data and data were selected by individual teams at their discretion and based on their sectoral focus, while pursuing the objective, purpose and methodology of the assessment. In principle, however, analytical work was used to evaluate the data obtained from the following sources: activity reports of competent authorities, regular and ad hoc evaluation and analytical reports, typological studies, SR's assessments prepared by international organizations, analytical documents prepared by the third sector and statistical data obtained through questionnaires from the representatives of relevant ministries and sectors in accordance with the requirements of the assessment tool. Relevant information was also obtained by analysing relevant primary and subordinate legislation, or managed discussions with relevant entities. It is not surprising that in the ex-post evaluation of individual NRA stages, collecting and gathering the necessary information belonged to predominantly one of the greatest challenges in the entire NRA process. This fact is also fully reflected within identified shortcomings or areas where relevant measures must be taken. In the context of the trend of the development of information technology, the commitment of the Slovak government to support the informatization of the society (including the central authorities of the state administration) and the fact that the 21st century is still around us, it is still incomprehensible that it is impossible to obtain all relevant information and unexplained discrepancies between the individual law enforcement authorities in identical statistical indicators.

Process independence of the organization of work in individual teams can be considered as one of the factors of successful completion of the whole NRA process. The specificities of each of the sectors allowed specific teams to set an internal system of work to reflect as much as possible the needs of individual members, both in terms of evaluation and in terms of performing other job responsibilities. The focus, intensity, length and modes of communication were tailored by individual teams to predetermined partial objectives and the timetable/work schedule, which was the result of mutual consultations between representatives of the NRA working group and representatives of the WBG. When looking back, the plan can be described as ambitious, given the typical Slovak circumstances accompanying the whole NRA process.

Two workshops were important part of the NRA process, according to the methodology. The planning of subsequent tasks and activities for a period of one calendar year was the sign of high professional level and attempt to achieve the most consistent results. An important element was the ongoing coordination of the process by the FSJ and MISO-LP. In Bratislava, in November 2017, the final NRA seminar was held under the auspices of the State Secretary of the Ministry of Interior SR. The representatives of the World Bank, the President of the Police Force, Deputy Prosecutor-General for criminal section, Special Prosecutor, Directors-General of the sections of Ministries and state institutions discussed the preliminary results and findings of the NRA, especially identified shortcomings in the activities of the competent authorities and the activities of the responsible persons. The purpose of the presentation of identified threats, vulnerabilities and gaps in the activity of the assessed entities was to motivate the management to initiate internal processes to introduce appropriate changes. Along with the identified shortcomings, the NRA working group also presented a detailed overview of the proposed measures, including responsible and co-responsible bodies, and the expected timetable for their implementation.

Tool for National Assessment of the Risk of ML and TF

The selection of a suitable tool for the practical implementation of the NRA was the key determinant of its successful completion and the achievement of relevant and especially useful results. Equally important selection criterion was also the acceptability by the competent bodies of the European Union and of the Council of Europe, mainly with regard to the system and assessment methodology. These assumptions were best met by WBG. This is already the second generation of assessment tools designed to eliminate as much as possible the adverse impact of the diversity of features of the national AML/CTF regime as well as the lack of relevant information and data in the country. Based on a discussion with the World Bank representatives, the relevant tool was tailored to the realities of the Slovak Republic in order to make the most of its potential, thereby achieving an added value. This related in particular to the modification of its focus on the concepts used in the Anglo-Saxon legal system, which, especially at the level of the law enforcement authorities, allowed for more efficient use of the currently kept statistical data.

The assessment of the national ML risk itself is determined on the basis of an assessment of:

- a) **threats** of the legalization of proceeds of crime at national level, and
- b) the level of **vulnerability** in relation to the legalization of proceeds of crime at national level.

In the context of the purpose of NRA, an assessment of "threats" is understood as an assessment of qualitative and quantitative information on the nature of income and proceeds derived from criminal activity or financing that were generated on the territory of the Slovak Republic or outside its territory. On the other hand, an assessment of "vulnerability" means assessing the shortcomings and weaknesses of the country's defence mechanism from the point of view of legalizing the proceeds of crime and terrorist financing.

The tool consists of a total of **nine modules** divided into two groups in terms of entering and subsequent evaluating qualitative and quantitative data and relevant information. The first group consists of modules that have unambiguous and relatively complex logic and apply weighted averages, built-in assumptions and formulae. This group includes a national vulnerability assessment module and modules designed to assess vulnerability in individual sectors. The second group consists of modules that are based on relatively simple matrix structures. These are modules for the threat assessment at national level, the assessment of the risk of terrorist financing, and assessment of financial inclusion products and services.

ML threat assessment module

- Helps determine the threat level at the national level, which is expressed in a five-point scale from "low" to "high". The aim is to identify the main predicate offenses, the origin and the flow of income (proceeds) derived from crime and the trends and procedures used for legalization in the Slovak Republic. The essence of the module

should facilitate the systemic collection of ML threat data and the analysis of cross-border ML threats. Part of the module is also the evaluation of income (proceeds) derived from criminal activity that is not recorded or have an unknown origin.

ML vulnerability assessment module

- Consists of an analysis of national defence against ML and also of the vulnerability of the relevant sectors. The value of the vulnerability is given by the numerical expression from "0.0" to "1.0" and the verbal description from "low" to "high",
- Internal scheme of the module is based on the understanding of causal links (causal relationships) between individual vulnerability factors related to the regulatory, institutional and economic environment of the Slovak Republic.

Evaluated factors in relation to the defence of the Slovak Republic for ML and counter-measures taken at national level:

- Quality of AML policy and strategy,
- Effectiveness of the definition of a criminal offense of legalization of proceeds of crime,
- Scope and comprehensiveness of laws on property seizure,
- Quality of collection and processing of intelligence information by FSJ,
- Capacity and resources for investigation of financial crime,
- Integrity and independence of the bodies responsible for detecting financial crime,
- Capacity and resources for prosecution of financial crime,
- Integrity and independence of the law enforcement authorities for financial crime,
- Capacity and resources for judicial proceedings,
- Integrity and independence of judges,
- Quality of border controls,
- Complexity of the customs procedure in relation to the transport of cash and liquid financial instruments,
- Effectiveness of customs controls in relation to the transport cash and liquid financial instruments,
- Effectiveness of cooperation at national level,
- Effectiveness of cooperation at international level,
- Availability of an independent audit,
- Level of financial integrity,
- Effectiveness of tax collection,
- Level of formalization of the national economy,
- Availability of credible identification infrastructure,
- Availability of independent information sources,
- Availability and access to beneficial ownership information.

Evaluated factors in relation to individual national economy sectors:

- Complexity of the AML legislation,
- Effectiveness procedures and the practical performance of supervision and control,
- Availability and enforceability of administrative sanctions,
- Availability and enforceability of criminal sanctions,
- Integrity of the staff of obliged entities,

- Effectiveness of compliance⁴ functions,
- Effectiveness of monitoring and reporting suspicious activities,
- Market impact on compliance with AML standards,
- Availability and access to beneficial ownership information,
- Availability of credible identification infrastructure,
- Availability of independent information sources.

The basic step in the evaluation of the above factors was the use of the so-called manuals that included an explanation of the nature of a particular factor; the criteria usable in the evaluation, and the possible (recommended) sources of information. After weighing the individual criteria, the specific factor was assigned a final rating. The necessity for the rating assignment was its sufficient justification based on available and ant "evidence" and, in particular, on the objectivity of the evaluation team. The final ratings thus obtained were then inserted in the pre-prepared excel files that were part of the NRA tool that processed them through defined conditions and built-in formulae. By combining the results of the national defence capability and the vulnerability of individual sectors, the overall final level of national vulnerability was reached. At the same time, a list of areas that needed to be addressed by the competent authorities, was drawn up. The aim is to help the relevant authorities in the decision-making process, identifying the needs that need to be addressed with priority based on the current state and development of the national AML and CTF system.

TF risk assessment module

- Systematically consists of three analytical sub-modules. The first area, as a prerequisite for assessing the risk of terrorist financing, was focused on assessing the level of the terrorist threat itself for the Slovak Republic based on a detailed analysis of qualitative and quantitative information related to the SR and data related to the investigated terrorist acts. The second area already focused on analysing and evaluating the direction, resources and channels designed/usable for TF purposes. Within the third area, the strengths and weaknesses of the defence mechanisms were assessed, especially the quality of legislation, coordination mechanisms, personnel and organizational provision of protection against FT, as well as the quality of TF policies and strategies and operational procedures.

⁴ Compliance: a set of measures adopted by a particular entity to ensure compliance with the applicable legislation

PART 1 – RISK OF LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY

CONTEXTUAL FACTORS OF THE SLOVAK REPUBLIC IN RELATION TO LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY

The Slovak Republic as an independent country was established on 1 January 1993 by the split of the Czech and Slovak Federative Republic. For the 25 years of independent existence, the Slovak Republic has undergone an intensive transformation process, which was characterized mainly by increasing the performance of the national economy and growing foreign investment. The driving force of these changes was an attempt for creating an economic environment that would be able to cope or compete with the developed countries of the European region. The result of this effort is the membership of the Slovak Republic in the EU since 2004. Another step in the integration of the Slovak national economy into the European Union was the introduction of the single European currency EURO and therefore the accession to the European Monetary Union in 2009. For this reason, the Slovak Republic as a Member State must meet high standards in the protection of the internal market, internal market transactions, and must have adequate legislative and institutional measures in place.

A steady increase in the GDP resulted in an improvement of other macroeconomic indicators such as labour productivity growth and competitiveness. Despite the negative effects of the economic crisis in 2009 and at the turn of 2012 and 2013, the increase of geopolitical risks and the high dependence of the national economy on the import of primary energy sources, the SR has been among the most dynamic growth rate within the EU Member States over the last ten years, as well as in Europe. From the point of view of macroeconomic indicators, GDP per capita in purchasing power parity is 77% of the European average and shows a continued increase. The long-term unemployment rate is decreasing and has historically reached the lowest level (in 2017, at 8.1%). Household consumption and foreign demand have the greatest impact on these indicators, which speeds up the export activity. Also, the year-on-year growth of the minimum wage (and average wage) was recorded. Compared to the V4 countries, the SR ranks second in the performance of these macroeconomic indicators. Recently, a decline in inflation rates and a reduction of the government deficit and the general government gross debt have been reported. The recorded level of these macroeconomic indicators is a promise of balanced economic growth from the point of view of both domestic and foreign demand and investment over the next period. Balanced economy is expected in the light of the general government budget deficit. It was just the consolidation of public finances that increased the pressure on the elimination of the shadow economy, which is its part despite everything and impairs the integrity and stability of the market as well as of the relevant institutions. According to the OECD estimates, it has a decreasing trend, still being at 1.63% of GDP⁵ in 2017.

Despite the above aspects of positive economic development as well as the geographical location, the SR is not considered as a country where it is worth to place income and proceeds from crime. The country has no "appropriate" legislative and institutional

⁵ For more details, please see EUROSTAT

conditions that would motivate foreign perpetrators of criminal offenses against property and criminal offenses of economic nature to do so, i.e. from the point of view of international legalization the country is not perceived as a significant country. This conclusion is also confirmed by the findings and results of the currently submitted NRA.

OVERALL LEVEL OF THE RISK OF LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY

Overall level of **ML RISK** in the conditions of the SR is MEDIUM-HIGH (MH)⁶.

Overall level of ML risk is determined by the following facts:

- a) Overall level of **ML THREAT** - MEDIUM-HIGH LEVEL (MH) and
- b) Overall level of **ML VULNERABILITY** - MEDIUM-HIGH LEVEL (MH).



⁶ L – low, ML – medium low, M – medium, MH – medium high, H – high

1.1. THREAT OF LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY AT NATIONAL LEVEL⁷

1.1.1. GENERAL ASSESSMENT OF THE THREAT OF LEGALIZATION OF PROCEEDS OF CRIMINAL ACTIVITY

The first step in the process of detecting the ML risk level in Slovak Republic conditions is the identification of facts which may and predominantly cause damage to the state, the public and the national economy. At the same time, it is necessary to diversify them in terms of their seriousness and possible impact on the legitimate interests of the Slovak Republic. The result of such an approach is the preparation of adequate countermeasures to mitigate or completely eliminate these facts.

The overall level of the ML threat in SR conditions is "medium-high" ("MH") with an increasing trend. The extent of unrecorded proceeds of criminal activity not sanctioned by criminal prosecution is substantially higher.

Geographical factors affecting the overall level of threat:

- National ML threat: "high" – "H"
- Foreign ML threat: "medium-high" – "MH"
- Unidentified origin of ML threat: "medium-high" – "MH"

After the initial application of the World Bank's tool, the expert group of the team for threats identified the limits of the relevant module. Apart from the fact that it is based on the concepts used in the Anglo-Saxon system of law (this fact was manifested in the very demanding subsuming of the currently kept statistical data by the law enforcement authorities in the area concerned⁸), it was shown very soon that the result of the particular analysis based on an insufficient scope and low quality of the legally convicted cases of legalization of proceeds of crime for the relevant period (for example, initiated but not finalized criminal prosecution cases for the given period are absent) could have only limited conclusions that would weaken the explanatory power of defining threats and would not use the potential of the NRA evaluation mechanism.

For the purpose of identifying the complex ML threat in the Slovak Republic, the relevant tool was supplemented by an analysis of other factors, in particular the overall development of crime and also the current characteristics and expected trends of criminal activity. The Working Group focused on creating cohesive quantitative and qualitative indicators with the highest explanatory power. An important factor was the incorporation of the impact of the analysis of the potential for generating illegal income in the context of unreported crime, the

⁷ **These are just the key findings to which the general public has access. The document, which contains a detailed analysis of the individual factors, including statistical data, assessment of the typology and trends in crime, is fully accessible for service purposes to police bodies, prosecutor's offices of the ministries concerned and the National Bank of Slovakia.**

⁸ This fact was most striking in the field of awareness of the scope of prosecution (e.g., division into the investigation and prosecution phases) or seized proceeds of crime

extent of which was affected mainly by the intensity of formal and informal inspection, the tolerance of the injured, the level of legal awareness, the type of crime, etc.

In determining the threat of the level of unreported crime, the Working Group chose the following assessment:

- the ratio of unrecorded proceeds is not significant
- the ratio of unrecorded proceeds is slightly higher,
- the ratio of unrecorded proceeds is higher,
- the ratio of unrecorded proceeds is substantially higher,
- the ratio of unrecorded proceeds cannot be estimated.

Based on this comprehensive approach within the threat assessment module, the Working Group identified:

- **General sources of threats - the areas of crime generating the largest scope of crime proceeds and related major predicate offenses,**
- **Identification of the extent of unpunished legalization of proceeds of crime and**
- **Follow-up trends and procedures used to legalize proceeds of crime - forms of placement and ways of concealing the origin of funds from criminal activity.**

A more detailed assessment with the expression of the general ML threat of a specific predictive offense is as follows:

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium-low	Low	Without change	Increasing	Falling
Criminal violence	except for carrying concealed weapons and arms trafficking, where the ratio of unrecorded proceeds is substantially higher, the ratio of unrecorded proceeds for criminal violence is not significant				X				X
Premeditated murder § 144	not significant					X			X
Murder § 145 (old § 219)	not significant					X			X
Robbery § 188 (old § 234)	not significant				X		X		

Extortion § 189 (old § 235)	not significant				X				X
Duress §§ 190, 191 (old §§ 235a, 235b)	not significant					X			X
Carrying concealed weapons and arms trafficking § 294 (old § 184a)	the ratio of unrecorded proceeds is substantially higher		X					X	
Carrying concealed weapons and arms trafficking § 295 (old § 185)	the ratio of unrecorded proceeds is substantially higher		X					X	

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium-low	Low	Without change	Increasing	Falling
Moral crime	Except for human trafficking, where the ratio of unrecorded proceeds is substantially higher, the ratio of unrecorded proceeds for moral crime is not significant				X			X	
Procuring and soliciting prostitution § 367 (old § 204)	the ratio of unrecorded proceeds is substantially higher			X			X		
Manufacturing of Child Pornography § 368 (old § 205b)	the ratio of unrecorded proceeds cannot be estimated					X	X		
Dissemination of Child Pornography § 369 (old § 205c)	higher				X			X	

Possession of Child Pornography § 370 (old § 205d)	not significant					X	X		
Human trafficking §179 (old § 246)	substantially higher			X				X	

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium	Medium-low	Without change	Increasing	Falling
Criminal offenses against property	Ratio of unrecorded proceeds is slightly higher			X					X
Theft § 212 (old § 247)	slightly higher			X					X
Failure to Pay Wages and Redundancy Payment § 214 (old § 248a)	not significant					X			X
Unlawful Enjoyment of a Thing of Another § 215 (old § 249)	not significant					X			X

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
--------------------------	---	-----------	--	--	--	--	-------	--	--

		High	Medium-high	Medium	Medium	Medium-low	Without change	Increasing	Falling
Criminal offenses of economic nature	ratio of unrecorded proceeds is (disproportionately) higher			X				X	
Embezzlement § 213 (old § 248)	not significant			X					X
Unlawful Manufacturing and Enjoyment of Payment Means, Electronic Money or Other Payment Card § 219 (old § 249c)	not significant			X			X		
Fraud § 221 (old § 250)	higher			X			X		
Credit fraud § 222 (old § 250a)	higher				X				X
Insurance Fraud § 223 (old § 250c)	higher					X	X		
Subsidy Fraud § 225 (old § 250b)	higher			X			X		
Unjust Enrichment § 226 (old § 250d)	not significant					X	X		
Fraudulent Bankruptcy § 227 (old § 250e)	substantially higher			X				X	
Induced Bankruptcy § 228 (old § 250f)	higher				X		X		
Usury § 235 (old § 253)	substantially higher, its volume not so significant			X			X		

Forgery, Fraudulent Alteration and Illicit Manufacturing of Money and Securities § 270 (old § 140)	slightly higher				X		X		
Tax and Insurance Evasion § 276 (old § 148)	higher	X						X	
Failure to Pay Tax and Insurance § 277 (old § 148a)	higher		X				X		
Tax fraud § 277a	higher	X							X
Failure to Pay Tax and Insurance § 278 (old § 148b)	higher			X			X		
Counterfeiting and altering a public instrument, official seal, official seal-off, official emblem and official mark § 352 (old § 176)	not significant					X	X		
Abusing participation in economic competition § 250 (old § 149)	higher					X	X		
Unlawful Business Activity § 251 (old § 118)	higher or substantially higher				X		X		
Unlawful employment § 251a	not significant					X	X		
Unlawful Trading in Foreign Currency and Providing Foreign-Exchange Services § 252 (old § 118a)	not significant					X	X		

Breach of Regulations Governing Imports and Exports of Goods § 254 (old § 124)	not significant			X		X		
Breach of Regulations Governing the Handling of Controlled Goods and Technologies §§ 255, 256, 257 (old §§ 124a, 124b, 124c)	not significant				X	X		
Distortion of Data in Financial and Commercial Records § 259 (old § 125)	higher		X			X		
Damaging Financial Interests of the European Communities § 261 (old § 126)	higher	X				X		
Endangering Trade, Bank, Postal, Telecommunication and Tax Secrets § 264 (old § 122)	not significant				X	X		
Insider Trading § 265 (old § 128)	higher			X		X		
Deceitful Practices in Public Procurement and Public Auction §§ 266, 267, 268 (old § 128a, 128b, 128c)	higher	X					X	
Harm Cause to a Consumer § 269 (old § 121)	not significant				X			X
Unfair Trade Practices § 269a	not significant				X	X		

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium	Medium-low	Without change	Increasing	Falling
Criminal offences of corruption	ratio of unrecorded proceeds is higher		X				X		
Misuse of office by a public office-holder § 326 (old § 158)	higher		X				X		
Passive Bribery § 328 (old § 160)	higher		X				X		
Passive Bribery § 329 (old § 160a)	higher		X				X		
Passive Bribery § 330 (old § 160b)	higher			X			X		
Active Bribery § 332 (old § 161)	higher		X				X		
Active Bribery § 333 (old § 161a)	higher		X				X		
Active Bribery § 334 (old § 161b)	higher			X					X
Trading in Influence § 336 (old § 162)	higher		X				X		
Election corruption § 336a	higher			X			X		
Sports corruption § 336b	/			/					/

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
--------------------------	---	-----------	--	--	--	--	-------	--	--

		High	Medium-high	Medium	Medium	Medium-low	Without change	Increasing	Falling
Organized crime	the ratio of unrecorded proceeds is substantially higher	X					X		
Establishing, Masterminding and Supporting a Criminal Group § 296 (old § 185a)	substantially higher	X					X		
Smuggling of Migrants § 355 (old § 171a)	substantially higher		X					X	
Smuggling of Migrants § 356	substantially higher		X					X	

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium	Medium-low	Without change	Increasing	Falling
Drug-related crime	the ratio of unrecorded proceeds is substantially higher		X					X	

Illicit manufacturing and possession of narcotics or psychotropic substances, poisons or precursors, and trafficking in them § 171 (old § 186)	not significant					X		X	
Illicit manufacturing and possession of narcotics or psychotropic substances, poisons or precursors, and trafficking in them § 172 (old § 187)	substantially higher	X						X	

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium	Medium-low	Without change	Increasing	Falling

Cybercrime / computer crime in a broader sense	the ratio of unrecorded proceeds is substantially higher	X						X	
--	--	---	--	--	--	--	--	---	--

Crime / criminal offence	Estimated amount of unrecorded proceeds	ML threat					Trend		
		High	Medium-high	Medium	Medium	Medium-low	Without change	Increasing	Falling
Legalization of proceeds of CA from registration statistical system EŠSK	the ratio of unrecorded proceeds is substantially higher		X					X	
Sharing § 231 (old § 251)	substantially higher			X			X		
Sharing § 232 (old § 215a)	substantially higher					X	X		
Legalization of proceeds of criminal activity § 233 (old § 252)	not significant		X					X	
Legalization of proceeds of criminal activity § 234 (old § 252a)	not significant					X	X		

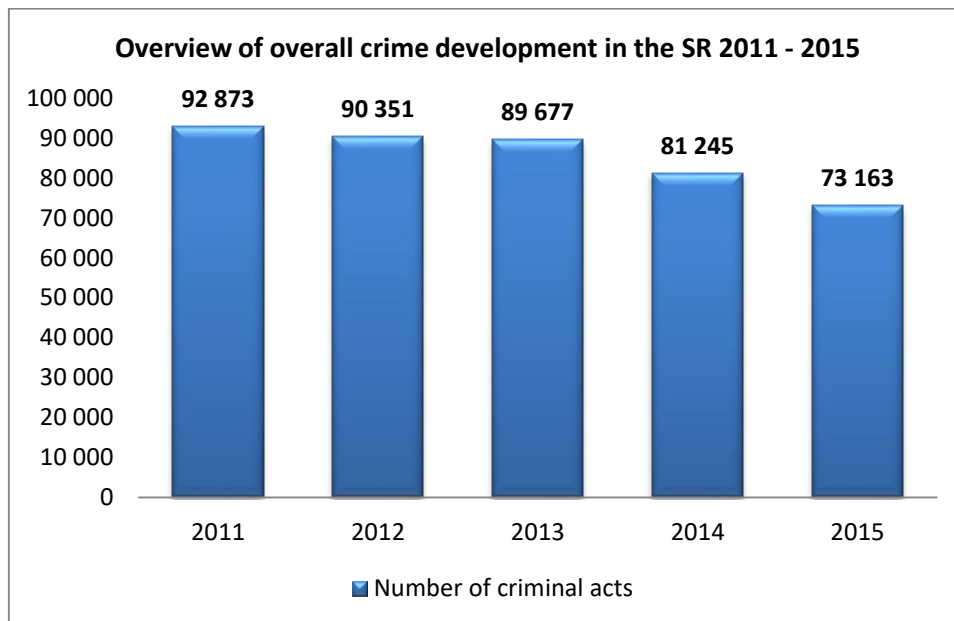
1.1.2. ASSESSMENT OF THE BASIC SOURCE ML THREATS ARISING FROM THE SPECIFIC TYPES OF CRIMINALITY AND THE RELATED FORMS OF CRIMINAL ACTS

The **baseline prerequisite** for assessing the threat of legalization of proceeds of crime is the **understanding of the overall context of the long-term development of crime** in the conditions of the Slovak Republic and its impact and factors influencing the extent and volume of generation of the proceeds of crime.

It is necessary to be aware of a wide range of factors that have an impact on the commission of criminal acts. In terms of ML threats, however, it is primarily the motive of the perpetrators in the form of generating profits (proceeds), i.e. the reason why the relevant

offense is committed by them, and the **determination of the potential of the type of criminal acts.**

The development of the security situation in the territory of the Slovak Republic in terms of the number of detected crimes can be considered as extremely positive. There has been a **marked drop in the overall incidence of criminal acts; thus, we can talk about the gradual trend of reducing** the overall incidence of offences.

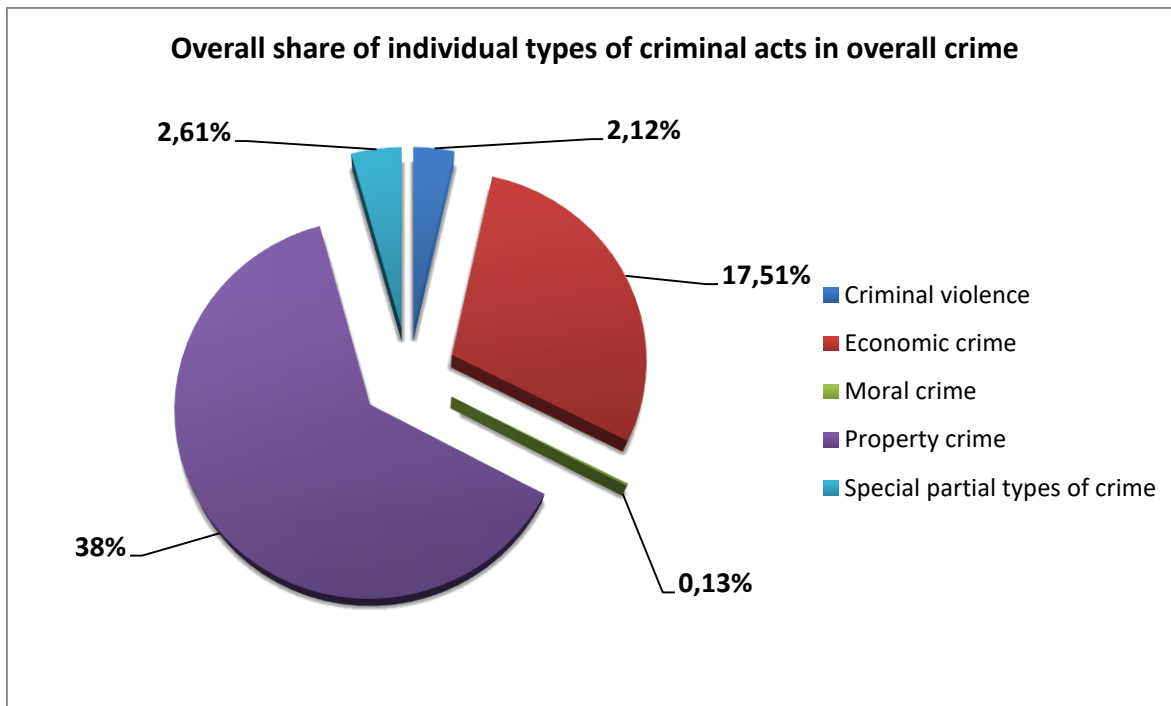


From the point of view of identifying ML threats, it is important to **distinguish between individual types of criminal acts, while for the needs of the NRA, the offences generating the highest damage were identified from the individual types of criminal acts⁹, which were then considered in the individual statistical data.**

For the purpose of identifying and evaluating the threats posed by the individual types of criminal acts and the related forms of crime, the following have been specifically analysed:

- Criminal violence
- Moral crime Criminal offenses against property
- Criminal offenses of economic nature, and
- Special partial types of crime:
 - Corruption-related crime
 - Drug-related crime
 - Organized form of committing crime
 - Cybercrime.

⁹ The issues of relationship between the damage and the proceeds of crime are discussed below.



CRIMINAL OFFENSES AGAINST PROPERTY

ML threat for Criminal offenses against property is medium with a declining trend. The ratio of the level of unrecorded proceeds is slightly higher, but the significant ML factor is the fact that the percentage is almost 50% of the total prosecution of persons in the SR¹⁰. Damage identified for Criminal offenses against property is 28.38 % of the identified damage for overall crime in the period under review.

The offence of theft (in particular high-value things and organized forms) still has the highest potential for generating proceeds whose expected unrecorded income is slightly higher.

Long-term theft of high-value things, mainly motor vehicles and machines is of particular importance in relation to **ML threats**. There is also a **well-organized form (especially recorded since 2013)** of this crime, particularly in the case of stealing goods transported by freight car transport, but also burglary within dwellings and recreational facilities.

For Criminal offenses against property, we may notice **ML threats related to the use of information and telecommunication technologies** (including social networks and online payment platforms), internet banking, and the like.

Given the assumption of the persistence of a higher degree of latency in Criminal offenses against property, the **threat of legalizing proceeds from this type of crime will be at the same level as it has been so far, will have a slightly accelerated trend.**

¹⁰ The number of prosecuted persons, despite its dominant position, has a **markedly declining trend**, between the order of 24 436 (2015) and 38 211 (2011) persons. **Percentage of total prosecution of persons is almost a half of all prosecuted persons, about 49.24%** with a stable trend

CRIMINAL OFFENSES OF ECONOMIC NATURE

ML threat for criminal offenses of economic nature, **especially with regard to the amount of damage caused (total damage caused by criminal offenses of economic nature amounts to 1,622,352,000,- EUR, which accounts for a 60.49 % share of the total damage) and to the detection rate of economic criminal acts, is in the range of 50.03% to 60.55% in the period under review; it is medium-high to high with a constantly unchanging trend, with the expected amount of unrecorded income being (disproportionately) higher.**

ML the threat for tax offences (most frequently, recorded crimes in the said type of criminal act¹¹) is medium-high to high. The expected amount of unrecorded proceeds or the amount of benefits received is disproportionately higher than for the reported criminal activity. Despite the measures taken, due to the constant transformation of the modus operandi of these crimes, the trend of the ML threat is without change, except for the tax and insurance evasion, which has an upward trend.

The application of excess deduction of value added tax has an important potential of ML threat, and also criminal activity in the form of carousel fraud is a continuing threat with an upward trend.

The ML threat resulting from the misuse of the forms and schemes of companies must be considered as especially high, where there is a significant disproportion between detected and latent crime. This typology also has significant cross-border spillovers. The volume of identified proceeds generated is significantly lower than the one actually generated without conducting a proactive financial investigation. The so-called CEO fraud represents a significant level of ML threat with an upward trend in terms of the method of committing crime and the ratio of undetected volume of generated proceeds. The essential feature is the conduct, which also shifts this type of crime into the sphere of the so-called Cybercrime.

In cases where straw men are used, in particular due to **the absence of documentary evidence and proactive, parallel investigation**, the documentation of criminal activity is very demanding and, **as a rule, those who have the greatest benefit from such conduct are not criminally punishable, which represents the extraordinary potential of ML threat.**

In the period under review, **the number of fraud cases in the freight transport of goods grew, which has an immanent cross-border character. The volume of proceeds generated by fraud in international freight transport is difficult to estimate, but it represents a higher rate than reported crime; from this point of view, there is a significant potential of the ML threat with a constant and/slightly declining trend.**

¹¹ In 2011 – 2015, a total of 23 211 tax offences was detected, out of which 16 706 were detected. In relation to total crime, tax offences had a 5.43% and the state budget suffered from a **loss of 637,858,000,- EUR, which accounts for a 2378% share of the total loss of prosecuted crime.** The incidence of tax offences represents a **31.03% of the share of criminal offenses of economic nature.** In the period under review, there were 2,515 cases of convictions (a 10.84% share) from the total number of tax offences, and in one case, the punishment of the confiscation of a thing was imposed. The forfeiture of property was not imposed.

In harming the financial interests of the European Communities, ML threat is medium-high with a rising trend.

From among other criminal acts of this type of crime, income generating threats have a significant potential:

- **Tax and insurance evasion** (high threat, increasing trend, the ratio of unrecorded proceeds is higher),
- **Failure to pay tax and insurance** (medium-high threat, trend without change, the ratio of unrecorded proceeds is higher) and
- **Fraudulent bankruptcy** (medium threat, increasing trend, the ratio of unrecorded proceeds is substantially higher),
- **Usury** (medium threat, steady trend, the ratio of unrecorded proceeds is substantially higher).

For Criminal offenses of economic nature, we may notice **ML threats related to the use of information and telecommunication technologies** (including social networks and online payment platforms), internet banking, and the like.

Given the assumption that Criminal offenses of economic nature in the Slovak Republic will have an increasing trend, the related ML threat will be progressive. The highest potential for generating profits from Criminal offenses of economic nature will have in particular tax crime, whereas its organized and sophisticated form is expected.

PARTIAL TYPES OF CRIME

o ORGANIZED CRIME

The ML threat level for organized forms of crime remains high, especially with regard to the volume of proceeds generated, the volume of unidentified proceeds, the nature, social danger and the extent of related crime in predicate offenses with a balanced trend, but with a transformation in the area of type crime, with a significant shift to Criminal offenses of economic nature.

In recent years, organized crime has learnt the lessons and moved its activities from the so-called racketeering, violent and drug-related crime to more sophisticated and profitable forms that are more complicated to detect and convict the perpetrator.

From the point of view of prognosis of the development, **it can be assumed that the organized forms of crime generating the largest volumes of illegal income, such as tax fraud, smuggling or illegal supplies of high-tax goods, trafficking in human beings, will become more intensive. Certain potential of the ML threat must also be noticed in connection with illicit arms trafficking.**

There is still a ML threat in the organized form of smuggling of migrants, also in view of the volume of unidentified proceeds generated by this crime. The increasing trend in the

import of labour from the Balkans and the related potential of organized crime mainly with respect to important business entities, will have to be considered as a threat.

The organized form of crime will continue to pose a permanent ML threat with an unchanged amplitude of the trend but with a marked change in the nature of the crime committed towards Criminal offenses of economic nature.

○ CYBERCRIME

The most serious forms of cybercrime in a broader sense **represent a significant ML threat with a growing trend. The ratio of unrecorded proceeds is substantially higher.** Recorded cyber-attacks overcome the conventional crime, becoming a horizontal element of its commission. **The existence of digital currencies represents a special threat with a growing trend.**

Cybercrime as a horizontal element of crime is a relatively new type of crime in the Slovak context. The most serious forms of cybercrime represent a significant ML threat with an increasing trend.

A low detection rate of cybercrime has a strong connection with the development of new information technologies and services related to the use of various sophisticated methods in P2P/TOR networks, etc. Despite the constant incidence of criminal acts, we recorded still low % detection rates of the offence of damage and misuse of a record on a data carrier. In the case of damage caused by cybercrime, its share of the total crime was steady in 2011 - 2015.

For Criminal offenses against property and Criminal offenses of economic nature, we may notice **ML threats related to the use of information and telecommunication technologies** (including social networks and online payment platforms), internet banking, and the like. **Encryption of communication**, which is a clear trend, facilitates the commission of crime. **Phishing, using malware and ransomware** are still present.

In 2011 and 2012, a significant **growth of online fraud and its modifications** was reported. In 2014 and 2015, perpetrators predominantly used event-specific forms of committing Criminal offenses of economic nature consisting in the so-called **“redirecting payments“ within standard business payment system of business partners in high volumes (in the order of millions of EUR).**

The ML threat resulting from the existence of virtual currencies¹² is high with an increasing trend also with respect to the scope of the unidentified volume of such placed proceeds of crime.

Given that **these ML threats and risks do not have a local but cross-border nature**, which is linked to the global expansion and Internet access as well as connectivity facilities, these threats and risks require an international approach both at FIU level as well as within

¹² **Slovakia is the second country in Europe where it is possible to buy and sell the Bitcoin virtual currency in a shop.** Just as it is possible to top up the credit, starting from 1 September 2016, it is possible to use one of 41 shops of the GECO network as a bitcoin exchange office.

banking systems, but also **cooperation with the providers of telecommunication services (including social networks).**

In the case of cybercrime, it will be possible to monitor in the future its high latency in committing crimes on social networks, in the so-called cyberspace. It is also possible to identify the rise in the link to the black economy, with the volume, whereas the extent and material damage caused by cybercrime will be high with a growing trend. An important ML challenge is to ensure the training of staff and create technical conditions required for its effective detection.

○ **DRUG-RELATED CRIME**

Drug-related crime is a **highly organized, lucrative and especially latent form of crime.**

From the point of view of generating proceeds of crime, we **can talk about a medium-high ML threat with an increasing trend**, with the expected amount of unrecorded proceeds being considerably higher.

No major changes are expected in the projected development of drug-related crime. **The SR is a country with a fully developed domestic drug market, where all drugs available in the European Union are offered. A significant factor in the increase of the ML threat is the fact that in the recent years, in the field of drugs, the Slovak Republic has changed from the transit country to the country of destination – consumption.**

Illegal proceeds from drug-related crime of transnational crime are legalized in Slovakia mainly by investing in services - cafes, restaurants, etc. Plus, they are investments in gambling establishments that are used to subsequently legalize the illegal proceeds, or real estate transactions through co-operating persons (dummies). The profits of Slovak organized crime involved in this type of crime are legalized/paid out also in the form of invoicing of fictitious services to companies engaged in retail services (e.g., rental of movable and immovable property) which control the persons involved in drug-related crime.

Organization is typical mainly of the Vietnamese community (methamphetamine, plants of the genera Cannabis (cannabis)) and the Albanian community (cocaine). People of Slovak nationality are mainly distributing methamphetamine and Cannabis plants. The importance of drugs trafficking into Europe by the "Balkan Route is growing, with most routes running through Slovakia and further spreading to Western European target countries towards end-users.

There is a presumption that the trend of introducing new psychoactive substances to the consumer market will continue. These are imported primarily from Poland, Hungary and the Czech Republic, or they are shipped from East Asian countries. Clearly the highest priority of controlling the black market for narcotic drugs and psychotropic substances will be the penetration into the so-called cyberspace and monitoring of the illegal dealing in controlled substances on the Internet. An increase can also be expected in the so-called pharmaceutical crime and abuse of Internet pharmacies. The Slovak Republic will further be significantly affected by the regional factor of drug-related crime.

- **CORRUPTION in a broader sense**

In terms of the **threat of generating proceeds of crime, corruption represents a medium-high level of ML threat, with no significant fluctuations in its trend, mainly with reference to the fact that the expected amount of unrecorded proceeds is, given their character, certainly higher than the identified proceeds within the really prosecuted corruption offenses. In this context, however, it is extremely difficult to estimate the extent of unreported crime or the volume of resources coming from such activity.** However, only a major systemic corruption is the real ML threat.

According to the findings of the Working Group that correspond to the outcomes of the OECD Assessment Report, despite the fact that the FSJ reported a significant amount of reports of suspected legalization of proceeds of crime, in the period under review, LEAs focused on small “fast action” cases of corruption, and not to major and more sophisticated cases where the cases of foreign bribery can be included, and did not monitor at all the related proceedings of the legalization of proceeds of crime. In addition, except for a few exceptions, most of the cases of conviction of corruption in Slovakia is for low bribes. Investigators and prosecutors concentrate their resources on the cases where they can catch perpetrators "at work". Only exceptionally, there are positive examples of investigating only historical events and cases where high bribes and socially significant processes occur.

Reporting corruption and providing qualified evidence is one of the neuralgic points of the whole process. The social perception of still poor level of protection of corrupt crime notifiers is an extraordinary challenge in detecting and investigating corruption.

The trend of the ML threat in the field of corrupt behaviour in relation to the procurement of a matter of general interest remains unchanged. Healthcare is a long-term problematic area with frequent occurrence of corruption. The threat of generating proceeds from overestimated prices of projects funded by the euro funds, thereby generating illegal proceeds by invoicing fictitious services and other defects of processes within subsidy schemes, remains latent. Also, with respect to a relatively low number of convicted persons for corruption in public procurement, usually they are persons who are regular employees of contractors or entrepreneurs who were bidding for contracts, the ML threat related to public procurement processes will continue.

CRIMINAL VIOLENCE

From the point of view of the overall ML threat of criminal violence, we can talk about **a medium-low threat with a decreasing trend.** However, except for **carrying concealed weapons and arms trafficking**, where the ratio of unrecorded proceeds is substantially higher than the value of detected proceeds, the ML threat of this specific activity is **medium with an increasing trend** of its development with respect to the potential of generating proceeds of crime.

- **Extortion**

In this context, it is necessary to **perceive the medium-low level of ML threat** only in the cases of serious crimes of **extortion prosecuted within the subject-matter and local jurisdiction of the Specialist Prosecution Office of the Public Prosecutor's Office of the SR**. It involves primarily the **members of criminal groups, because extortion remains one of the ways in which they get illegal profits**. However, the ML threat trend is declining.

In general, it is possible to predict that criminal violence will continue to play a marginal significance in relation to the possible generation of proceeds of crime and their subsequent legalization, without any significant change in the trend. However, an organized form of committing certain types of criminal violence (e.g., extortion) still must be considered an ML threat.

Particular attention should be paid to the aspect of combating the **illicit manufacture, possession and trafficking of weapons, projectiles, ammunition and explosives**.¹³ The level of ML threat for this type of crime is medium-high with a prospective predicted growth. The level of ML threat for robbery is medium-low without any change in trends.

MORAL CRIME

From the point of view of the ML threat, **mainly human trafficking** (in particular, forced begging, forced marriage, sexual and labour exploitation¹⁴) has a **potential to generate proceeds of crime, for which the ratio of unrecorded proceeds is substantially higher than the value of detected proceeds, taking into this fact, the ML threat is medium, and the development trend is increasing**.

Procuring and Soliciting Prostitution is a latent form of this criminal activity, which is **identified and detected only to a minimum extent**. A specific type of this crime is the so-called "escort service".

Although the volume of proceeds generated from prostitution is hard to estimate, it is not a high ML threat, where its threat is only present in its links to organized crime, without significant fluctuations in trend.

From the offence of **child pornography**, the **dissemination of child pornography has a low ML threat with an increasing trend**, as the estimated unrecorded amount of proceeds is hard to estimate, but certainly higher than for the reported crime.¹⁵

¹³ From the point of view of long-term statistical reporting and with regard to the nature of the offense, this type of crime is included in criminal violence.

¹⁴ Based on an analysis of prosecutions initiated over the last four years, trafficking for the purpose of sexual exploitation (almost 50% of cases) prevails. Forced begging is the second (about 20% of cases), followed by labour exploitation (about 15% of cases) and the remainder are forced marriages and combinations of the above exploitation purposes (about 15% of cases).

¹⁵ Since investigators dealing with the detection of this type of crime during the period under review did not receive support in a proactive parallel investigation, there is a lack of identification of proceeds in this area, as well as the actual provision and collection of the proceeds of this crime by the perpetrators. With regard to the nature of child pornography, it is statistically difficult to determine the damage and therefore does not appear in the statistics of this crime. Therefore, it is not real to estimate the volume of perpetrators' proceeds.

In general, an **increase in commercially motivated moral crime** (procuring and soliciting prostitution, trafficking in women and children, etc.), which is the source of illegal proceeds, can be expected, and therefore it will represent the highest ML threat of this type of crime. The impact and importance of the Internet for the expansion of moral crime, which is a significant ML threat, will continue to grow.

1.1.3. ASSESSMENT OF THREATS ON THE BASIS OF LEVELS AND QUALITY OF DETECTION, INVESTIGATION AND CRIMINAL PROSECUTION OF THE CASES OF LEGALIZATION OF PROCEEDS OF CRIME

The quality of the actually investigated and prosecuted criminal offenses of the legalization of proceeds of crime under Article 233 of the Criminal Act did not reflect the seriousness and extent of the predicate criminal offenses detected.

Despite the rising trend in the use of preventive tools in the form of seizure of proceeds of crime in the preliminary procedure, the final seizure of proceeds through property decisions was minimal or zero.

The analysis clearly confirmed the fact that during the period under review there was an **inability to "demonstrate" the abundance of real convictions, seizure and confiscation of the proceeds of crime in so-called High Profile Cases.**

The insufficient quality and nature of actually investigated and criminally prosecuted criminal offenses of legalization of proceeds of crime was particularly evident in cases where predicate offenses included serious fraud, financial crime, tax crimes, serious criminal offenses against property, criminal activity committed through the forms of organized crime, corruption, abuse of power by a public official, and the like. Only a minimum number of cases of autonomous legalization or legalization by third parties - professional legalizers, was registered. Equally, the ML aspects of sophisticated forms of abuse of legal entities were sanctioned insufficiently or were not sanctioned at all.

The absence of a real proactive parallel financial investigation is the largest source of an ineffective system of detecting and generating serious cases of legalization of proceeds of crime.

ANALYSIS OF THE CASES OF LEGALIZATION OF PROCEEDS OF CRIME

The number of cases prosecuted did not change dramatically in the period under review of 2011 - 2015.

In the period under review of 2011 - 2015, police authorities assessed 1 165¹⁶ ML cases (the offense of the legalization of proceeds of crime and the offense of sharing), which represents only a 0.27% share of a total of 427 309 of all committed criminal acts.

¹⁶ The difference between the number of ML cases recorded in the registration statistical system for crime (1 278 cases) and the number of ML cases considered (1 165 cases) was due to a change in the legal

In connection with the offense of sharing and the offense of legalization of proceeds of crime (Articles 231, 232 and Articles 233, 234), the Prosecutor's Office, **for the period under review:**

- **Terminated the criminal prosecution of**
 - o **unknown persons in 775 cases**
 - o **known persons in 1 196 cases**
 - **out of it, in 714 cases, brought an indictment and in 179 cases, concluded a plea bargain, 75 x conditionally discontinued the criminal prosecution.**

According to MoJ SR's data, 487 persons were lawfully sentenced. When assessing only the offense of legalization of proceeds of crime under Article 233¹⁷ and Article 234 of the Criminal Act, the said statistical data are as follows:

- 607 cases assessed by police authorities (criminal prosecution initiated = 0.14 % share of all criminal prosecutions initiated),
- completed criminal prosecution of:
 - unknown persons in 621 cases,
 - knowns persons in 289 cases,
 - out of it, in 179 cases, brought an indictment and in 33 cases, concluded a plea bargain, and in 2 cases, conditionally discontinued the criminal prosecution.

According to MoJ SR's data, 40¹⁸ were validly convicted of the offense of legalization of proceeds of crime.

Basic overview of the quantitative indicators of the criminal prosecution of the legalization of the proceeds of crime during the evaluated period							
legalization/+including sharing § 233 (252), 234 (252a)/ +§§ 231 (251), 232 (251a)						TOTAL	Trend
	2011	2012	2013	2014	2015	2011-2015	
Number of postponed UTRs total	79	125	72	141	111	528	↕
Number of postponed UTRs by obliged entity / FSJ	72/79	122/125	71/72	139/141	109/111	513/528	↕

classification of the offense during the investigation (the difference in the initiation of the prosecution under Article 199 Criminal Act and bringing of indictment under Article 205 CA or another termination

¹⁷ Including offenses under the old Criminal Act (§ 252 and § 252a)

¹⁸ Even in the case of convicted persons there were significant discrepancies between the data of GPO SR and MoJ SR. GPO SR reports 638 convicted persons, out of it 91 convicted of the offense of legalization of proceeds of crime under § 233 or 234 of the Criminal Act. As all the final decisions at the level of the Ministry of Justice, which is officially responsible for this part of the statistics, were physically evaluated for NRA purposes, the working group decided to use MoJ SR's statistics.

Referral of postponed UTRs to LEAs	30	34	20/24	78	51	213/237	↕
Referral of information to FSJ with suspected ML for LEAs	150/150* ¹⁹	198/198*	131/136	300** ²⁰	221**	1000/1005	↕
Initiated criminal prosecution	140/296	145/277	106/256	111/239	105/210	607/1278	↕
Terminated criminal prosecution of unknown persons	101/133	116/143	128/161	118/151	158/187	621/775	↑
Terminated criminal prosecution of known persons out of it:							
	32/210	64/237	61/292	62/269	70/188	289/1196	↑
Conditional discontinuation of CP						2/75	
Accused persons	17/98	38/141	35/173	36/128	53/174	179/714	↑
Proposal of plea bargain	0/33	7/35	8/40	9/40	9/31	33/179	↕
Σ	17	45	43	44	62	212	↑
Discontinued CP	79/0	98/0	102/106	97/111	109/116	485/510	↑
Convicted persons	8/84	7/102	12/115	11/121	2/65	40/487²¹	↕

¹⁹ * In 2011 and 2012, sharing was together with legalization (2011, sharing 2x, 2012 sharing 3x)

²⁰ ** In 2014 and 2015, only § 233

²¹ The data are based on the number of valid decisions (judgments) sent by courts at the request of MoJ SR. Module 2 – vulnerability shows slightly different data (42/492) based on official statistics published on the MoJ SR's website

Postponement of proceeds € (all obliged entities)	710,273	1,933,116	830,870 / 858,058	3,980,117	3,179,166	10,633,542 / 11,491,600	↑
Seizure of proceeds (only money, €) within pre-trial proceedings – legalization/ other offences	14 / 293,308 / 740,363	15 / 204,999 / 2,029,716	20 / 8,811,287 / 29,818,213	31 / 756,080 / 8,505,901	20 / 4,585,683 / 4,418,543	100 / 14,651,357 ***22 / 45,512,736	↑
Of total €	1,033,671	2,234,715	30,023,212	7,283,229	9,004,226	49,579,053	↑
Final decision on confiscation of proceeds € - legalization/ all predicate offences	X	X	-/117,246	- /138,085	X	/255,331	↑

As for specific crimes generating the highest damage, here we include fraud, credit fraud, theft, embezzlement, tax and insurance evasion, tax fraud and failure to pay tax and insurance.

The following outcomes result from an analysis of **prosecuted cases** of the legalization of proceeds of crime (and also sharing) and the related nature of the identified proceeds :
 Even 71.93% ML acts are related to the predicate criminal offence of theft under § 212 of Criminal Act (mainly theft of motor vehicles or motorcycles, theft of a thing and theft by breaking and entering).
 The commission of predicate criminal offence of fraud (17.42%) follows. They were mainly the cases of unauthorized (fraudulent) transfer of funds for various products or services.
 The commission of offences with an international element was carried out only in cases involving theft of motor vehicles and fraud (unauthorized transfer of funds).
 For predicate criminal offences, the commission of offences in a sophisticated manner was not proved; to a negligible extent, predicate criminal offences were committed with respect to criminal violence.

²² *** It reflects data on seizure reported during the years to MONEYVAL

A large part - more than a half of the proceeds of crime is subject to the actual direct consumption of the predicate criminal offence perpetrators, without the specific elements of the legalization moment.

Legalization of proceeds of crime in prosecuted cases was carried out in particular by:
- transfers to bank accounts and by withdrawals from these accounts,
- sale of stolen and changed objects with the hidden origin of their acquisition from crime.

These conclusions are considerably distorted from the quantitative point of view, in particular due to the scope of the prosecuted legalization, the purpose of which was the legalization of stolen cars.

No sophisticated forms of legalization were identified, e.g. using the placement of proceeds abroad or with the involvement of professional legalizers.

In the case of organized forms of crime, the largest source of illegal proceeds in particular of criminal groups, is the economic, property, drug-related crime or a combination of these types of crime with criminal violence.

Based on experience in dealing with the legal cases with foreign countries, in general, it can be stated that most of the illegal proceeds arise from various types of **fraud committed through computer systems, that is, cybercrime in conjunction with the economic, cross-border nature**. In these cases, they are, for example, eliciting payments via the Internet for advertised goods, services, or for various reasons - credit, winnings, etc., transfers from accounts to foreign accounts without the knowledge of the holders, and others, with payments being directed to accounts abroad. In most cases, the cases are difficult to detect within the limitation periods of prosecution of criminal offenses.

IDENTIFICATION OF PROCEEDS AND WITHDRAWAL OF PROCEEDS

One of the baseline findings of the evaluation process is the fact that **there are no reliable statistical data** within the activity of LEAs and courts in the SR **that would quantify the value of the generated proceeds of crime with a sufficient level of explanatory power**. Such data are not systematically collected. One of the reasons is that determining the composition and amount of the proceeds of crime is a qualified process that is part of the evidence in a specific prosecution.²³

In the SR, however, we have systematically collected data on the amount of damage caused²⁴ for individual criminal offences, which are available to the P PF SR. This criterion, in

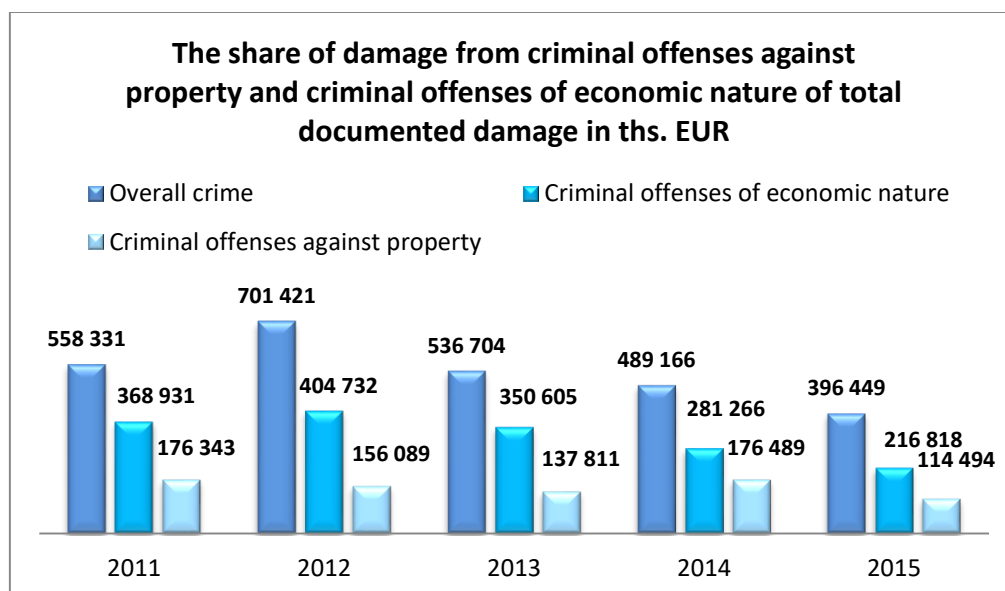
²³ Another problem is that the seizure itself contains its natural stages that are not statistically distinguishable (for example, an order to seize funds stated for a certain amount, a different amount is actually seized that can increase during the seizure), the seizure itself is performed in a qualified mode, and data should be uploaded to the information systems only after they have been declassified, thus creating space for statistical errors

²⁴ § 124 Criminal Act

(1) For the purposes of this Act, damage shall mean harm to property or actual loss of assets or prejudice to the rights of the injured party or other harm, which has a causal relationship with the criminal offence irrespective of whether the harm has been caused to a thing or to the rights. **For the purposes of this Act, damage shall also mean advantage gained in causal relationship with the criminal offence.**

the given context, provides an insight into the seriousness of the crime committed, as **damage is also understood as profiting in a causal connection to a criminal offense**. It is necessary to take into account that the damage in the system of criminal law in the Slovak conditions is a significant qualification factor determining the seriousness of the offense. In principle, however, it can be stated that **the amount of the damage is higher than the potential volume of the proceeds of crime**.

Based on the above described outcomes of the analysis of individual types of crime it can be stated that despite the fact that Criminal offenses against property have the dominant position in terms of the number of offenses committed, then **in terms of the amount of damage, unequivocally Criminal offenses of economic nature with a share of 60.49% prevails. In Criminal offenses of economic nature, just tax crime with a 3103% share has a considerable share. Criminal offenses of economic nature are followed by Criminal offenses against property with a 25% share.**



Statistical data show that the competent authorities seized only 12.24% of the value of value of the legalized property identified in the prosecution.

The analysed court decisions reveal that the **withdrawal of proceeds by direct instruments in cases of criminal prosecution of the legalization of proceeds of crime under § 233 of the Criminal Act was minimum or zero**. If, even in the period under review, the

(2) Damage within the meaning of paragraph 1 shall also mean the loss of profit to which the injured party, considering the circumstances and his personal situation, would otherwise be entitled or could reasonably expect to obtain.

(3) In case of criminal offences against the environment, damage shall mean the combined environmental harm and property damage; property damage shall also comprise the costs of restoring the environment to its original state. In case of the criminal offence of illegal handling of waste pursuant to *Section 302*, the scope of the offence shall be determined on the basis of customary price charged at the time and place of the offence for the collection, transport, export, import, recycling, disposal or dumping of waste, and the price charged for the removal of waste from the site that is not designated for dumping.

confiscation of a thing was imposed, it was generally an instrument for committing a crime, and not proceeds of crime. The confiscation of property was imposed exceptionally.

The proceeds of crime can be seized either by the forfeiture of property, forfeiture of a thing, or by imposing the protective measure for the confiscation of a thing, but in this regard **also by the imposition of a pecuniary penalty**. Because of its nature, the seizure of proceeds also includes the award of the **compensation of damage to the injured party in criminal proceedings, which is borne by the convicted person**.

The Slovak particularity is a relatively frequent imposition of a pecuniary penalty, which de facto withdraws the value of gained profit from criminal activity without the obligation of the judicial authorities to identify (and demonstrate) the specific things that were obtained by criminal activity or acquired for such things. Another advantage of this sanction is the relatively fast execution, as opposed to the lengthy process of confiscating a particular thing (or property).

The imposition of pecuniary punishment is, in terms of the withdrawal of proceeds of crime, the most important factor in the assessment of convictions for predicate offenses, for which due to the absence of a parallel financial investigation, criminal prosecution for the legalization of proceeds was not extended, and the criminal sanction of the perpetrator (either for self-laundering or for separate cases of legalization) was completed with such a process.

Without keeping statistical data on the value of pecuniary punishment imposed and the value of the compensation of damage awarded in criminal proceedings, it is not possible to demonstrate the effectiveness of this method of seizure of the proceeds of crime.

A frequent measure is also the **imposition of an obligation to compensate the injured party for damage**. However, if the damage cannot be quantified or accurately quantified, the injured party would have to refer it to a civil procedure. However, no statistical data are kept on how many injured parties actually made their claim in a civil procedure.

From the judicial decisions under review concerning the criminal prosecution of the legalization of proceeds of crime, **the compensation of damage was imposed in a total of 56 cases, the pecuniary punishment in 27 cases, and in 57 cases the injured party was dependent on a civil procedure**.

The concept of the **withdrawal of illegal proceeds outside criminal proceedings (without a previous conviction in criminal proceedings)** in the form of procedures according to Act No. 101/2010 Coll. **on proving the origin of property**, appears as **absolutely ineffective** now (without real results).

ML GEOGRAPHICAL FACTORS

A total of 1113 Slovaks participated in ML cases, which is a 95.54% share of the total number of ML cases (1165 cases) and foreigners appeared in 53 ML cases, number 99 (an 8.50%)²⁵.

Offenses with an international element were committed mainly in cases involving the theft of motor vehicles and fraud (unauthorized transfer of funds). It is clear from the analysis that statistically the proceeds generated in the Slovak Republic still prevail. However, from a qualitative point of view, an increasing trend of the detection and subsequent prosecution of money laundering with an international element with the generation of proceeds of crime, must be provided. This fact is significant not only in the context of a growing volume of prosecution of the so-called carousel fraud. As a relevant regional scope, it is possible to designate neighbouring countries, in particular the Czech Republic and Hungary. At some distance, Ukraine and Austria and Poland follow. The EEC countries are significant, particularly Italy, the Federal Republic of Germany, Switzerland and the Netherlands. Also, ML cases involving tax havens were not produced.

For the **target country** of ML cases it is important to determine the country in which things, proceeds or property should be placed after their/within the legalization or sharing. In the vast majority of ML cases, the target country was the SR (in 1059 ML cases, representing a 90.90% share). Among the other most frequently occurring target countries were Ukraine (20 ML cases, which is a 1.72% share), Poland (12 ML cases, 1.03%) and Hungary (8 ML cases, a 0.69% share). Most frequently, proceeds in the form of transfers of funds and stolen vehicles were directed to foreign countries.

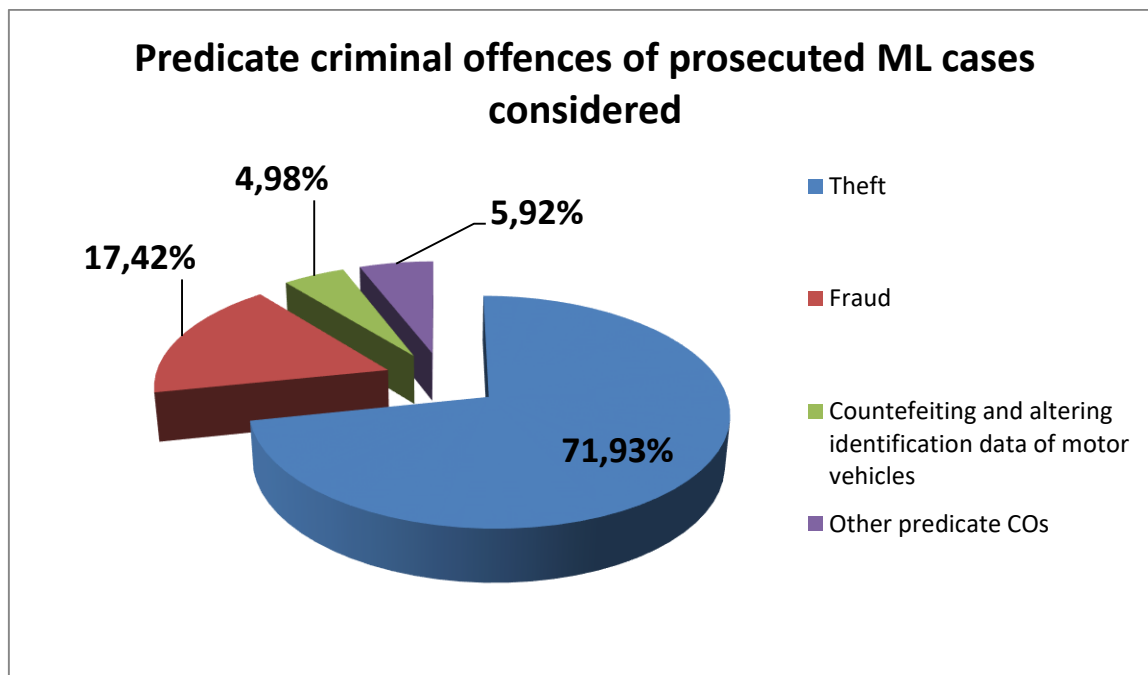
The most frequent target country for transfers of funds was Ukraine. It is interesting to note that such countries as China, Hong Kong, Cameroon, Russia, Serbia, Turkey, i.e. non-EU countries were target countries for this method.

Furthermore, there were ML cases with stolen vehicles, where the target country was again mainly Ukraine. ML cases with the consumption and repayment of false checks were directed to foreign countries less frequently.

In relation to the **country of origin**, for ML cases, the highest representation had the SR (63.52%), followed by Germany (8.50%), Austria (7.98%), Czech Republic (4.64%), % and other countries. In 74 ML cases the country of origin was not detected (6.35% - it was mainly related to car theft and subsequent legalization). However, the main threat is cybercrime.

RELATED PREDICATE CRIMINAL OFFENCES:

²⁵ For this characteristic of ML cases, it was taken into account how many persons were involved in legalization or in the sharing, i.e. how many people were suspected and how many people were accused.



Even 71.93% of the deeds constitute theft under § 212 of the Criminal Act (in particular the theft of a motor vehicle or a motorcycle, theft of things and theft by breaking and entering).

It is followed by the commission of predicate offences in the form of **fraud** (17.42%). These were in particular cases of unauthorized (fraudulent) transfer of funds for various products or services. Other predicate offences²⁶ occurred only marginally with a 5.92% share (from 0.09% for the offence of carrying concealed weapons and arms trafficking to 2.40 % for the criminal act of robbery).

In ML cases linked to criminal groups, these **systematically focused on fraudulent transfers of real property and their subsequent legalization, in terms of proceeds from this criminal activity, there were large financial proceeds, which in individual prosecuted cases exceeded the amount of EUR 1,000,000.** The investigation of such cases generally lasted from the start of the criminal prosecution until the submission of an indictment for at least 6 years.

The most widespread **form of punished legalization of proceeds of crime was found in the form of personal consumption of stolen things and funds.**

From the point of view of the services (products) used and the sectors and institutions involved, the analysis of all ML cases shows that most often it was about possession and use (37.17% of ML cases), then a bank (15.80 % of ML cases), district office (14.16% of ML

²⁶ Carrying concealed weapons and arms trafficking, tax and insurance evasion, failure to pay tax and insurance, abuse of power by a public official, establishing, masterminding and supporting a terrorist group, illicit manufacturing and possession of narcotics or psychotropic substances, poisons or precursors, and trafficking in them

cases), originality check (8.58% of ML cases), District Traffic Inspectorate (7.73%) and conventional sale (6.44% of ML cases). Other subjects appeared sporadically.

Sectors	ML threat for the sector					Trend		
	High	Medium-high	Medium	Medium-low	Low	Without change	Increasing	Falling
Banking, offshore		X					X	
Securities			X				X	
Asset companies				X		X		
Insurance sector			X			X		
Payment institutions, payment service agents and electronic money institutions		X					X	
Leasing				X		X		
Creditor					X	X		
Financial agent and financial advisor					X	X		
Exchange office			X			X		
Gambling operator	X					X		
Real estate agencies, building sector, development	X						X	
Health service, sale of medicinal products and medical materials	X						X	
Merchants with precious metals and stones		X				X		
Auditors					X	X		
Accountants				X		X		
Lawyers			X			X		
Notaries			X			X		

Tax advisor			X			X		
Pawnshops			X			X		
Auction					X	X		
Non-profit organizations		X					X	
Other services (advertising, sports, sponsoring ...)	X						X	
Others (cars, possession and use, standard sale, personal consumption, etc.)		X					X	

An assessment of the seriousness of predicate offenses and the related volume of money laundering shows that the most serious are: criminal acts in the area of tax crime, Criminal offenses of economic nature and Criminal offenses against property.

However, from a qualitative point of view, it is necessary to note the increasing trend of detection and subsequent prosecution of money laundering with the cross-border element of generating proceeds of crime. This is particularly important in the context of the increase in the volume of prosecution of the so-called carousel fraud.

In the relevant period, systematic measures taken at the level of GPO SR started to be visible. While in 2011, 2012, the dominant were prosecution cases the predicate offenses of the theft of motor vehicles and their subsequent legalization with VIN cloning or the consequences of simpler forms of fraud. Data from 2015 indicate the prosecution of more sophisticated forms of fraudulent conduct and mainly the accelerated prosecution in the field of cybercrime but also, for instance, in the field of fraud. **When assessing the nature of actually initiated criminal prosecutions (but not validly terminated), it is clear that this positive trend is growing.**

1.2. VULNERABILITY WITH RESPECT TO THE LEGALIZATION OF PROCEEDS OF CRIME AT NATIONAL LEVEL

The basic precondition for introducing effective tools and measures within the national AML and CTF system is to identify vulnerable and weak points and possible gaps that would facilitate potential perpetrators to place, stratify and integrate the proceeds of crime.

The overall level of vulnerability of the SR is based on the evaluation of two basic parameters:

1. Country's ability to combat ML,
2. Overall vulnerability of the sectors of the national economy.

The overall level of vulnerability of the country from the point of view of combating the legalization of proceeds of crime was determined at the level of **medium to medium-high** level - the score according to the programme tool : **0.6**.

The result of the country's overall ML vulnerability at national level points to the fact that the level of measures in combating money laundering is average and a **more problematic area is mainly the low effectiveness of these measures**. The reason for the weaker ability of the country to combat legalization is the lack of quality of search, detection of crime, the quality of prosecution, the quality of judgments and an impaired quality of the framework of the seizure and final confiscation of illegally acquired property. The resulting average level of overall sectoral ML vulnerability is primarily determined by the moderate vulnerability of the banking sector, which is the most important sector from among the evaluated ones for the national economy, and the financial sector of the country. Priority measures to strengthen the country's capability to fight against the legalization of proceeds of crime should primarily relate to capacity and resources to detect financial crime and the banking sector.

1.2.1 COUNTRY'S ABILITY TO FIGHT AGAINST THE LEGALIZATION OF PROCEEDS OF CRIME

In general, the ability of the country to fight against ML can be understood as the ability of the competent authorities to effectively prosecute and sanction the cases of the legalization of proceeds of crime, as well as the ability to identify and seize the income and proceeds arising from criminal activity. The country's ability to fight against ML was evaluated at a **medium-low to medium level** - the score according to the programme tool: **0.40**.

The country's ability to fight against ML is mainly influenced by the following factors:

Factors affecting the SR's ability to fight against ML	Score
Quality of AML policies and strategies	0.5
Effectiveness of the definition of the offense of legalization of proceeds of crime	0.6
Comprehensiveness of legal framework for seizure of property	0.6

Quality of the FIU's activity in obtaining and processing financial intelligence information	0.6
Capacities and resources for detecting and investigating financial crime	0.3
Integrity and independence of law enforcement units	0.6
Capacities and resources for criminal prosecution of financial crime	0.5
Integrity and independence of LEAs	0.6
Capacities and resources for judicial proceeding on financial crime	0.5
Integrity and independence of judges	0.5
Quality of border checks	0.7
Comprehensiveness of the customs procedure on the inspection of cash and similar money market instruments	0.7
Effectiveness of customs controls on cash transport and similar financial market instruments	0.7
Effectiveness of national cooperation	0.5
Effectiveness of international cooperation	0.7
Level of formalization of the national economy	0.7
Level of financial integrity	0.7
Effectiveness of tax collection	0.5
Availability of an independent audit	0.7
Availability of trusted identification infrastructure	0.5
Availability of independent information resources	0.5
Availability of information on beneficial ownership	0.5

QUALITY OF AML POLICY AND STRATEGY

- a Strategic Plan to Combat Money Laundering and Terrorist Financing for 2012 - 2016

The strategic plan was based on the need to take effective measures to identify the proceeds of crime and to prevent their placement in the market economy and further use, as well as to create conditions for their final confiscation. At the same time, it was necessary to point to the unwanted situation in detecting, investigating and prosecuting Criminal offenses of economic nature where, where in most cases, the LEAs document only predicate offenses and does not deal with income and proceeds generated by them. At the same time, A Schedule for Material and Time Implementation of the Measures from the AML and CTF

Strategic Plan for 2012 - 2016, was prepared. With respect to that the said Schedule was not discussed by the Slovak Government but was discussed at the MISO-LP level, which does not have instruments to enforce the obligations arising from the results and conclusions of the meeting. For this reason, the Strategic Plan did not have a positive impact on the development of crime, namely the detection of legalization of proceeds of crime or the detection of predicate offenses that generate the highest proceeds or income.

- Action plans to combat tax fraud

The fight against tax fraud is a long-term goal supported by the Slovak Government. For this reason, Action Plans to Combat Tax Fraud were adopted by resolutions of the Government of the Slovak Republic. The individual measures were strategically elaborated by individual units and departments, whether through a change in legislation or by adopting new internal procedures and methods. The implementation of the measures of the approved Action Plan to Combat Tax Fraud has brought relevant results and achieved the objective pursued. This involves in particular to reduce the scope of tax fraud and evasion, to identify them more quickly and to sanction the perpetrators more effectively. The negative impact of the implementation of measures is a change in the behaviour of a certain part of the business community in the sense that the form of fraud moves into more sophisticated forms.

In the period under review, a set of comprehensive measures based on risk assessment in the system of anti-legalization measures was not developed in the conditions of the SR.

Vulnerabilities:

- Obligated entities do not sufficiently assess the clients in terms of the risk of legalization and terrorist financing, even if the obligated entities identify a higher risk with the client, the subsequent measures to mitigate the risk of the client are not executed and the risk is not reduced to the acceptable level by obliged entities,
- The Strategic Plan to Combat Money Laundering and Terrorist Financing for 2012 - 2016 was not submitted for adoption to the Slovak Government, the Strategic Plan did not define the responsibility of authorities and specific tasks and deadlines for the obligations,
- The current organizational integration of the FSJ must be changed due to the importance and complexity of its tasks, as the FSJ:
 - a) Performs the tasks of the Central National Unit in the field of the prevention and detection of the legalization and financing of terrorism,
 - b) As the gestor of Act no. 297/2008 Coll., the FSJ will prepare further legislative proposals in the fight against the legalization and terrorist financing and will contribute significantly to the elaboration of the AML Strategic Plan,
 - c) In the next period, it should also be in the role of coordinator of national risk assessment, which should be accepted by other institutions.

EFFECTIVENESS OF THE DEFINITION OF THE OFFENSE OF LEGALIZATION OF PROCEEDS OF CRIME

On the basis of the analysis of the judgments carried out, as well as on the basis of the analysis of the GPO of the SR on the limitations of criminal prosecution of the legalization of

proceeds of crime, and further analysis of the prosecution of self-laundering, the evaluation team notes that the legislation does not contain any legal obstacles to prosecution in cases of the so-called self-laundering, autonomous laundering and legalization of proceeds through a third party. Nevertheless, the analysis of particular judgments has shown that the potential of the legislation has not been sufficiently applied in practice.

The evaluation team notes that the existing legislation does not contain any conditions that would imply a specific approach to proving objective and subjective aspects competed to other criminal offenses. The problem, however, remains to prove the actual proceeds of crime that differ from the damage caused in criminal proceedings and require a relatively high degree of identification. This is particularly important in the absence of a proactive, parallel financial investigation.

Vulnerabilities:

- As a possible source of vulnerability it is possible to identify the negligent conduct of perpetrators in relation to the legalization of proceeds of crime or demonstrating the fulfilment of the subjective aspect of the offense, especially in cases where the persons are part of or a component of the legalization scheme and are only misused to open a bank account, or only to send the received funds, or withdraw cash elicited in a fraudulent manner (frontmen).

EFFECTIVENESS OF CROSS-BORDER CASH CONTROLS

The risk of smuggling of cash and other non-monetary assets is low despite the geographical location of the SR as an EU border country (and the Schengen area). The physical land border with Ukraine is only 98 km long and highly orographically structured. A major part of the border forms uneven ground, legal crossing is only possible through 3 road border crossings and 2 railway crossings. Largest part of the border is mainly forest and part of the border forms watercourses. Since this border is the Schengen border, its physical security is at high level. The number of border crossings is small, and the capacities built at that border are sufficient and complemented by technical devices for identifying goods, including cash. At the border crossings there are both stationary and mobile means of identifying goods.

After the incidents with smuggling of cigarettes and people, the air border is secured by the AF SR through radars. Three international airports of the Schengen type with third countries are the other border, where the level of controls is at the required level and meets the European standards. The largest of them, the Bratislava Airport reinforced its capacities by developing a Travel Regime branch which primarily addresses the detection of smuggling of goods including cash and non-monetary assets. The customs office carries out checks for the performance of the duty to report and is entitled to require the necessary co-operation of the inspected persons.

In the period under review, the number of cash transfer notifications for individual years is fairly balanced.²⁷ Most of the notifications were made at the UA - SKK border crossing point, the number of notifications at airports is limited by the fact that few flights from/to

²⁷ Detailed information on cash transfer reports is provided in Section 3 Terrorist Financing Threat

third countries are performed at Slovak airports. Slovak citizens use the airports in Budapest and Vienna for flights outside the EU, as witnessed by the fact that Vienna found passengers with unreported larger amounts of cash in the past. The competent authorities have a system for verifying the reporting of cash transfers both at national and international levels.

During the period under review, the competent customs authorities imposed two penalty notices for failing to notify the cash transfer, which was subsequently detected by inspecting the luggage. In one case, the passenger admitted the transfer of cash at the request of a customs officer.

Vulnerabilities:

- A risk was identified as regards the possible use of cash transport through postal items or freight. Legislative measures need to be taken and the duty to report must be extended to the customs authorities for dispatching or accepting postal or other consignments from/to the Slovak Republic outside the territory of the European Communities, it is also necessary to impose an obligation on the persons concerned to allow the customs authorities to control such consignments.
- Absence of enhanced cooperation between the competent authorities,
- Mutual exchange of information, provision of guidance and training,
- Absence of adequate legislative and organizational measures to effectively seize suspicious funds

QUALITY OF FINANCIAL CRIME DETECTION

a) Activities of the FSJ

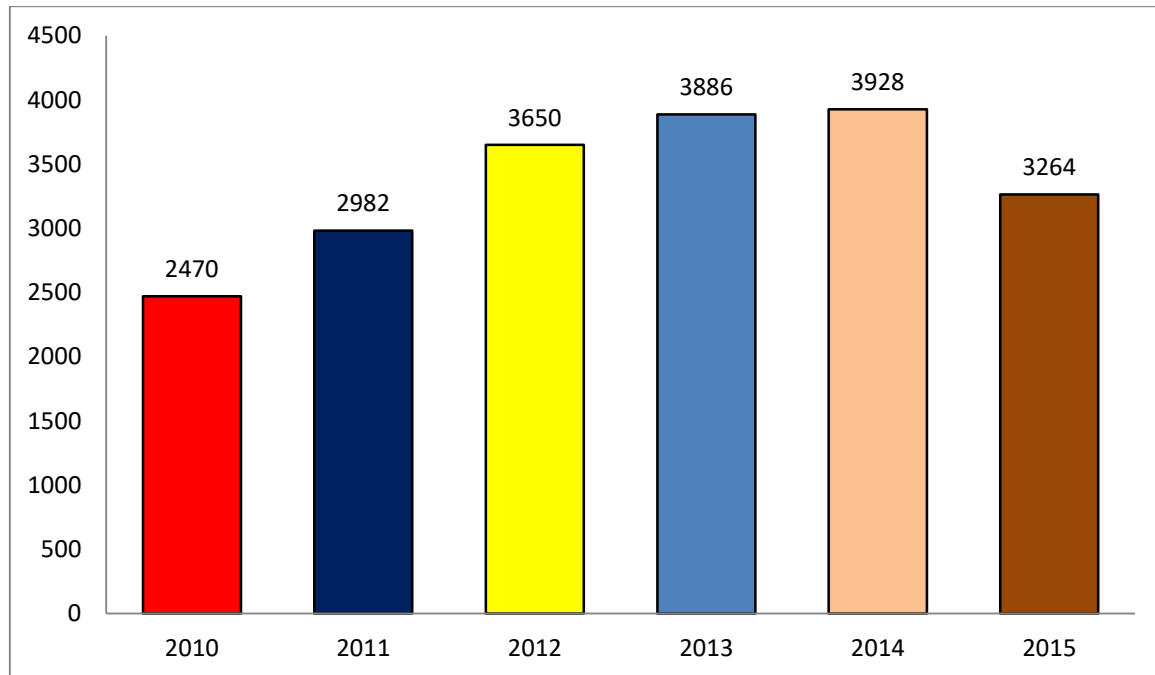
Since 2011, the MONEYVAL Committee has stressed its concerns about the FSJ's organizational status in the police structure and the system as a whole, which negatively affects the ability of the FSJ to bring ministries and other state bodies together for the effective functioning of the AML and CTF system. The MONEYVAL Council of Europe Recommendations also pointed out the need to increase personnel and material resources for the FSJ to strengthen its institutional position in the fight against legalization and terrorist financing, and not to weaken it. Problems in obtaining information in the framework of national risk assessment and changes in staffing within working groups have also shown an inappropriate institutional position of the FSJ (e.g., in the area of performance of its AML/CTF coordination function).

The FSJ is led by the director appointed by the director of the National Criminal Agency. The FSJ Director does not have the personal powers and the position of the FSJ Director is subject to high fluctuation. This is evidenced by the frequent personnel changes (five persons were in the post of the FSJ Director between 2010 and 2015), which has a negative impact on the FSJ's conceptual activity. Since the FSJ does not have its own budget, its material provision is not at an adequate level. FSJ police officers' earnings in the period under review did not correspond to either the average value of service salaries in other units within the NAKA; in the period under review, there was a reduction of service salaries due to measures resulted from the economic crisis. These facts have a negative impact in particular on:

- a) System for verifying UTRs,

- b) Implementation of strategic analyses and development of typologies, and
- c) system of exercising the FSJ inspection activity in relation to the performance of obligations of the obliged entities resulting from the AML/CTF Act.

Dynamics of the developments of UTR reports received in 2010 – 2015



Year	Total no. of Reports	type "A" ²⁸	type "B"	type "C"
2011	2 982	584	2 098	300
2012	3 650	565	2 586	499
2013	3 886	352	2 598	936
2014	3 928	501	2 414	1 013
2015	3 264	439	2 117	708
Total	17 710	2 441	11 813	3 456

UTR reports by the structure of obliged entities for 2011 - 2015.

²⁸ Report type „A“ – UTR reports with a high ML and TF risk, Report type „B“ – UTR reports with a medium ML and TF risk, Report type „C“ - UTR reports with a low ML and TF risk.

	2011	2012	2013	2014	2015
Banks	2,513	2,989	3,416	3,378	2,953
Insurance companies	-	258	155	174	112
Central Securities Depository	2	-	-	1	4
Management company and depository	23	23	41	64	30
Securities dealer	10	7	2	19	-
Supplementary pension company	2	-	-	-	1
Legal entity/natural person - exchange activity	1	120	116	8	9
Legal entity/natural person - trading in receivables	4	120	-	-	1
Legal entity/natural person- financial leasing	72	-	-	25	20
Payment institution	-	-	-	-	53
Gambling operator	49	45	12	6	22
Postal service undertakings	120	89	105	108	54
Court enforcement officer	-	-	-	-	1
Lawyer or notary	2	2	15	1	3
Legal entity/natural person - courier services	-	-	-	-	1
Legal entity/natural person - real estate business	1	85	1	1	-
Auditor	1	4	3	-	-
Accountant	3	-	-	-	-
Total number of UTR reports	2,982	3,650	3,886	3,928	3,264

In the period between 2011 and 2015, the FSJ provided 1,741 pieces of information to LEAs, of which 1,000 cases were referred for criminal prosecution in connection with a suspicion of legalization of proceeds of crime, out of which in 518 cases PF investigators initiated criminal prosecution under § 199 of the Code of Criminal Procedure, in 118 cases, an indictment was brought under § 206 of the Code of Criminal Procedure, 154 persons were accused, and a total of 40 persons was convicted.

- a) For an offence under § 233 Legalization of proceeds of crime – 75 cases,**
- b) For an offence under § 233 Legalization of proceeds of crime in parallel with an offence under § 221 Fraud – 6 cases**
- c) And in 7 cases an indictment was brought under § 206 of the Code of Criminal Procedure for an offense under § 233 Legalization of proceeds of crime – 5 cases, and for an offence under § 221 Fraud - 2 cases).**

The number of referred cases of the legalization of proceeds of crime varied during the period under review; the highest was in 2014 and the lowest in 2013.

For the period under review, as predicate offences for such referred information, there

were **868** cases of a suspicion of fraud (§ 221), **6** cases of a suspicion of sharing (§ 232, § 231), and **51** cases of a suspicion of another offence

- § 171 Illicit manufacturing and possession of narcotics or psychotropic substances, poisons or precursors, and trafficking in them,
- § 212 Theft,
- § 213 Embezzlement,
- § 219 Unlawful Manufacturing and Enjoyment of Payment Means, Electronic Money or Other Payment Card,
- § 220 Falsification and Fraudulent Alteration of Motor Vehicle Identification Numbers,
- § 222 Credit fraud,
- § 225 Subsidy Fraud,
- § 226 Unjust Enrichment,
- § 228 Induced Bankruptcy,
- § 236 Concealment of a Thing,
- § 251 Unlawful Business Activity,
- § 270 Forgery, Fraudulent Alteration and Illicit Manufacturing of Money and Securities,
- § 276 Tax and Insurance Evasion,
- § 277 Failure to Pay Tax and Insurance,
- § 352 Counterfeiting and altering a public instrument, official seal, official seal-off, official emblem and official mark.

Although the FSJ always requires feedback from LEAs on the use of the information sent and obtained within UTR reports, the feedback from the LEAs was not at the required level. In the period under review, no cooperative activities identifying problem areas and causes, were performed.

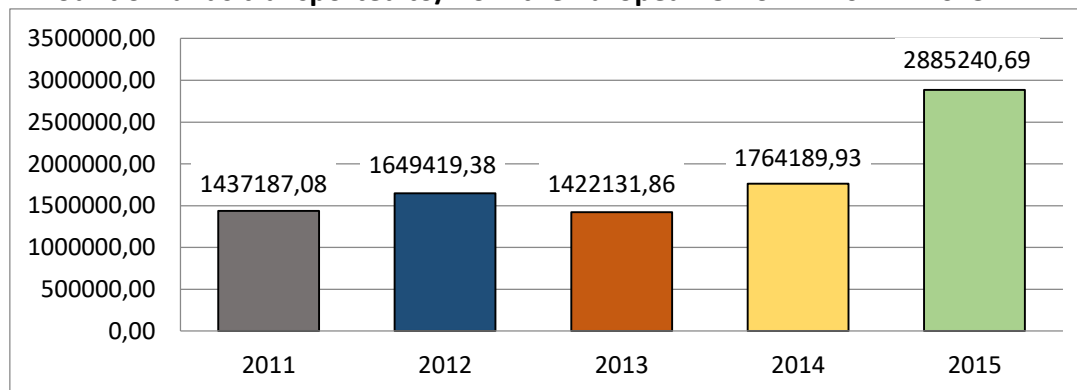
The customs office sends notifications of the cross-border transfer of cash to the FSJ on a monthly basis, in accordance with Article 4 par. 2 of Act No. 99/2004 Coll. of the Customs Act and on amending and supplementing certain laws, as amended (hereinafter: "Act No. 99/2004 Coll. the Customs Act") and notifications of committing a customs delict or a customs offence according to the provisions of Article 72 par. 1 n) of Act No. 99/2004 Coll. the Customs Act committed by a person who had provided false information on/had not reported the import, export or transport of cash according to Article 4 par. 2 of Act No. 99/2004 Coll. the Customs Act. Information received from cash transfer notifications is reviewed in the performance of FSJ activities and, based on the results of the analysis, it is referred to the competent authorities in the Slovak Republic or the FSJ partner services abroad or is entered into the FSJ internal database for further service use.

Overview of the cash transfer notifications to/from the European Union received by the FSJ and the amount of money transferred in 2011 – 2015:

Year	Number of reports received	Amount of transported funds in EUR
-------------	-----------------------------------	---

2011	66	312 637
2012	63	1 649 419.38
2013	58	1 422 131.86
2014	59	1 764 189.93
2015	72	2 885 240.69
2011 - 2015	318	8 033 618.86

Amount of funds transported to/from the European Union in 2011 – 2015.



b) Capacity and resources for detecting crime

In the conditions of the SR, operational units of the PF, operational units of the Financial Administration Criminal Office (FACO), FSJ according to a special regulation²⁹ and intelligence services are responsible for the detection of property and Criminal offenses of economic nature. In the case where the FSJ or intelligence services obtain information that may be related to criminal activity, they are obliged to forward the information to the competent PF unit having local and subject-matter jurisdiction or to the FACO. Under the Act on the Police Force, information and technical means and operational activities of search may be used in the performance of tasks in the field of combating the legalization of proceeds of crime. In the detection of tax evasion or illegal financial transactions or the legalization of proceeds of crime and related offenses and their perpetrators, an important legal entitlement for police officers of the Financial Police and Criminal Police Service is the possibility to ask for information in writing which is subject to bank secret.

Despite the fact that the above-mentioned criminal activity causes high damage to the national economy as well as to the property of the citizens and the state, in Slovakia, there is still no specialization in the area of detection of the legalization of proceeds of crime, especially in the absence of specialized services dealing with the so-called financial investigation. This fact also results in sufficient seizure and confiscation of proceeds and

²⁹ AML/CTF Act

income of crime (and the compensation for inflicted property or economic damage). At present, these acts are carried out by investigators investigating predicate offenses or criminal offense of the legalization of proceeds of crime. The vulnerability is very strong in this case, and this long-lasting undesirable condition must change.

A deficiency is the fact that no central register of bank accounts is established, and the detection of information that is subject to bank secret is more time-consuming due to the need to send requests to all banks, it is also not possible to track online account movements. Slovakia does not have a sufficient legal basis for property monitoring, in practice it is possible to detect how property is disposed of only through reinvestigation of the status, using repeated lustrations, sending new applications, and the like, whereas it is not active property tracking in real time.

c) Effectiveness of international cooperation

International cooperation at FIU-FIU level

The performance of international cooperation on the exchange of financial intelligence and other relevant information and data to combat ML and TF is fully implemented by FSJ members. To this end, two secure information channels are used, i.e. Egmont Secure Web and FIU.NET. Only members of the FIUs have access to the information exchanged through the channels. The determining element of the international exchange of information is given by the AML/CTF Act. The determining element of international cooperation is the so-called Principles of the Egmont Group for Information Exchange between Financial Intelligence Units that provide in detail the conditions for the provision and exchange of information and recommend the form of information requests. The effectiveness of international cooperation in verifying UTRs is, from the point of view of the SR, primarily determined by the scope of authorization of the foreign partner financial intelligence unit in obtaining and providing the requested information on behalf of the FSJ.

In the reference period of 2011 to 2015, the FSJ sent 1491 requests in the process of exchanging information abroad, and a total of 1138 requests for information was received and handled from abroad. The FSJ received 571 spontaneous information from abroad and sent 1950 spontaneous information abroad.

International police cooperation

On the part of police forces, international cooperation is developed at the required level, with the exception of cooperation with some countries where delays occur. LEAs cooperate with foreign partners under the Police Force Act, which stipulates that the Police Force cooperates with the police of other countries, international police organizations, international organizations and organizations operating in the territory of other countries in the form of exchange of information, exchange of liaison officers or other forms. This therefore constitutes the legal basis for providing international police cooperation.

In the field of the investigation and detection of criminal activities, the competent departments of the Police Force of the Slovak Republic use the national centres EUROPOL, INTERPOL, SIRENE, joint liaison officers and police attachés deployed in selected EU

countries and outside the EU. Part of the system is the efficient use and ability to set up joint investigative teams for demanding cross-border cases (the so-called JITs).

d) Availability of reliable information and evidence

d1) Level of formalization of the economy

According to research, more than one third of companies in the Slovak Republic are exposed to the competition of informal or unregistered companies, which represents a significant restriction in business. Companies that successfully avoid taxes gain a significant competitive advantage. The issue of tax evasion is one of the biggest problems of the shadow economy. VAT fraud performed as part of carousel transactions and the use of straw men play a major role in the shadow economy .

Compared to the EU, the size of the shadow economy in Slovakia can be considered average, but its size in the Slovak Republic cannot be described as negligible. The volume of the shadow economy in the Slovak Republic is gradually falling. Starting from 2008, there has been a decline from 16% to 14.1% in relation to GDP. In 2015, the volume of the shadow economy was estimated at 14.1% of the economic performance, while the average of the Member States was 18.5% of the economic performance. As a result of the shadow economy, every year, Slovakia loses tax revenues for 2.7% of GDP, roughly 2 bil. EUR. The shadow economy is most evident in the building industry, retail, wholesale, but also in agriculture, manufacturing industry, transport, accommodation, small services and restaurants³⁰.

In order to reduce the size of the shadow economy, it is necessary to focus on its causes rather than on its implications. The reasons are especially complicated regulation and high tax burden, which allow the growth of the shadow economy, a significant difference in the economic performance of individual regions of Slovakia and the related differences in the population's living standards. No less important is also the intensive use of cash in business.

d2) Reliability of financial records and books

Reliability of accounting records/books assesses whether ML investigators can rely on financial records/books to track the flows of financial proceeds of crime in cases of legalization of proceeds of crime. Reliability of financial records/books is affected by the level of financial integrity, the efficiency of tax collection and the availability of independent audit.

Investigators cannot always rely on corporate financial records to track the flow of money in investigating ML cases. The information provided by the banking sector is reliable, but the problem of monitoring the flow of funds arises in the collection of cash. It is problematic to find out how the funds were handled according to legal entities' accounting records due to the inconsistent keeping of accounts by entities committing criminal activity.

1. Level of financial integrity

In order to identify the level of financial integrity of business entities operating in the Slovak Republic, it is necessary to change the system of obtaining the relevant data and information. Based on currently obtained data, the level of financial integrity cannot be accurately defined. However, the competent authorities have a clear picture of the shortcomings and problems in the tax area. In order to remove and streamline tax collection,

³⁰ Source: see more EUROSTAT

an Action Plan to Combat Tax Fraud (including its update) was issued. One of the effective tools is the joint project of FA SR, NAKA in cooperation with the GPO SR - the so-called Tax Cobra. This project has introduced new control mechanisms and has greatly increased the level of cooperation of the competent authorities in the detection of tax crime, especially in cases of unjustified excessive VAT deductions.

Overview of the activity of the Tax Cobra since its creation on the basis of statistical data collected by the PF SR (NJFP NAKA P PF).

	No. of cases	No. of accused persons	Damage in EUR	Funds saved in EUR	Imprisonment	Valid judgment	
						Qualification	Sentence
Total 2011 - 2016	82	328	361,271,255.10	84,774,183.00	20	2 x § 277 Crim. Act Failure to Pay Tax and Insurance	Imprisonment 3y./PO 5y., Imprisonment 12 y. + fin. penalty 30,000,- EUR + prohibited to run a business 10y. + confiscation of 1,800,000,- EUR

In the context of Criminal offenses of economic nature, invoices and accounting documents are misused frequently, in particular forgery of these documents. This is also linked to inadequate business ethics and non-performance of obligations arising from supplier and customer contracts and agreements. Business ethics is continually developing in Slovakia. Successful companies, in the interest of promoting corporate culture, most often use training for newly-recruited employees to quickly adapt and orientate themselves in their companies. Companies apply different approaches to introducing basic ethical principles into economic practice. Companies with foreign participation, however, have developed codes of conduct, which take the form of a written document defining the basic principles of ethical behaviour applicable to the entire company.

2. Effectiveness of tax recovery

The tax burden in Slovakia is low, and mandatory contributions an important source of revenues. In Slovakia, the tax-to-GDP ratio is 31% of GDP, which makes Slovakia one of the countries with the EU's lowest tax burden. In 2014, taxes accounted for around 80% of all revenues, which is one of the lowest figures in the EU. The composition of tax revenues was relatively stable over time and was largely supported by mandatory contributions (Section 2.3), with income taxes and property taxes comparatively low. Although taxes on production and imports (e.g., VAT) as a share of GDP are below the EU average, for Slovakia it is the second largest source of revenues.

Anti-fraud measures for tax have contributed to improving tax collection. As part of the Action Plan to Combat Tax Fraud, the Government has implemented ca. 50 measures since 2012. The most important of these included the VAT control statement and the mandatory VAT advance on registration for high-risk applicants. The effective VAT rate rose from a record low figure in the third quarter of 2012 and stabilized at around 14.5% in recent quarters. The Ministry of Finance estimates that in 2013 – 2014, the effectiveness of VAT collection brought additional VAT receipts of 1.2% of the GDP, mainly due to the anti-fraud measures. The next period showed further improvements in tax collection. However, the continuing high outages in VAT receipts indicate that there are shortcomings in the tax discipline of VAT.

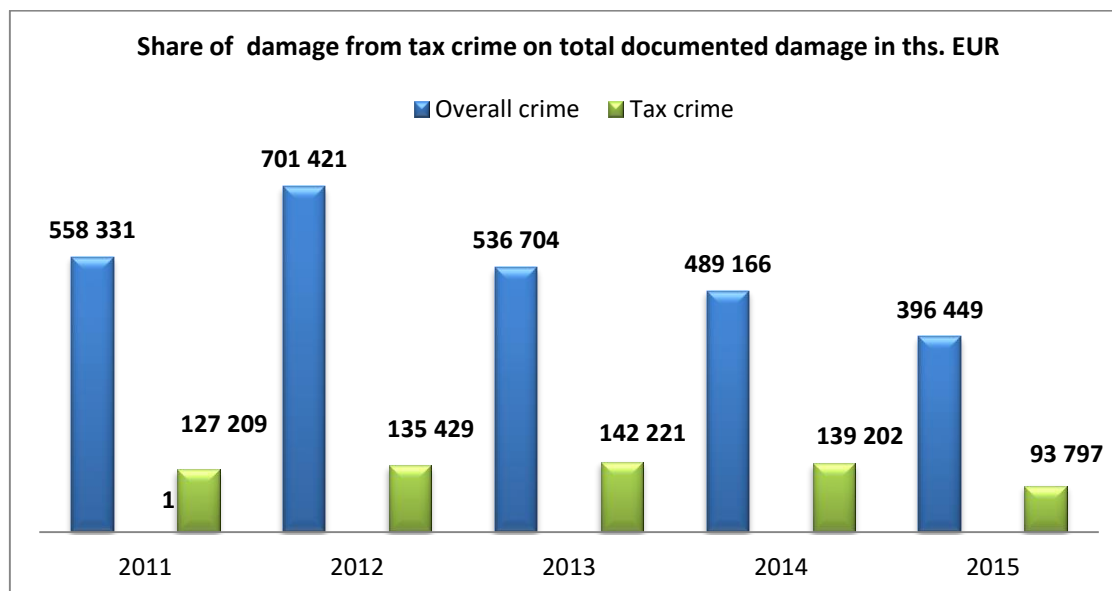
With respect to the volume of estimated tax evasion, it is clear that the current capacities of the Financial Administration for the implementation of the control activity are not sufficient. Of the total number of more than 9,000 employees in the Financial Administration, the inspector's position is carried out on the average by 1,500 employees. The Slovak Republic adopts various instruments aimed at reducing the demandingness of the control activity of the tax administrators and at adopting the possibility of highly effective targeted control with the removal of motivation factors for the infringement of legal regulations - the Action Plan to Combat Tax Fraud. The retention period of the employees in the position can, on the one hand, represent stabilization and expertise, on the other hand, it may be part of undesirable inertia and the risk of corrupt behaviour. Higher fluctuation has been recorded in Bratislava in the long term. The system of civil service relations does not include a system of employee rotation, therefore, they stay in the post to which they were hired, unless individual changes occur that cause a change in the civil service relation.

The direction in terms of streamlining the collection of taxes and duties is based on the plans of the Government of the SR defined in the Government Program Statement, for which one of the background documents is the Europe 2020 strategy, and on the objectives of the Ministry of Finance SR. Important documents for setting targets for more effective tax and customs tax collection include the Concept for the Reform of Tax and Customs Administration Reform with a View to Unifying the Collection of Taxes, Customs Duties and Insurance Contributions, the Concept of the Fight against VAT Tax Fraud, as well as other related documents. The aim in the area of tax and customs collection effectiveness is to continue the implementation of the reform plans of the Government of the Slovak Republic and the Ministry of Finance related to the process of unifying the collection of taxes and customs duties or collecting insurance contributions, including the continuation of the efficiency of FA activities. Strategic objectives, plans and specific tasks aimed at making Financial Administration's activities more effective are defined in the Financial Administration Development Concept for 2014-2020, which is based on the Strategy for the Development of Financial Administration prepared by the Ministry of Finance SR. The Financial Administration Development Concept for 2014-2020 provides an insight into what direction the Financial Administration will take in the next period.

A majority of the training of tax inspectors focuses on UNIVERSAL education in tax laws (procedural and substantive tax law), accounting, tax control procedure and control process, financial and economic analysis, fight against tax evasion and fraud. ESPECIALLY in relation to the topic of "combating money laundering and terrorism" - in particular corruption and

fraud. The above stated type of training is organized mainly through specialized courses or e-learning.

Between 2011 and 2015, a total of 23,211 tax offenses was identified, out of which 16,706 were clarified. Due to the above criminal activity, the loss of 637,858,000, - EUR was caused to the State budget. The incidence of tax offenses has a 31.03% share of Criminal offenses of economic nature.



3. Availability of independent audit

Statutory auditors and audit firms have conducted audits according to the International Standards on Auditing. The Act No. 423/2015 Coll. on Statutory Audit and on amendments and supplements to Act No. 431/2002 Coll. on Accounting, as amended (hereinafter: the "Statutory Audit Act") in Article 19 - International Standards on Auditing, as well as the previous Act No. 540/2007 Coll. on Auditors, Audit and Oversight of the Audit Performance and on amendments and supplements to Act No. 431/2002 Coll. on Accounting, as amended (hereinafter: the "Act on Auditors") in Article 20 – Audit documentation, imposes on statutory auditors and audit firms to respect the International Standards on Auditing issued by the IFAC (International Federation of Accountants), a member of which is also the Slovak Chamber of Auditors, in the conduct of statutory audit.

Violation of auditors integrity

According to the decisions of the Disciplinary Commission of the Slovak Chamber of Auditors for the years 2010 - 2015, the following violations of the Act on Auditors were committed:

Article 29 par. 5 - continuous training - failure to attend at least 120 hours of educational activities during a three-year cycle = 36 auditors,

Article 37 par. 2 - rights and obligations of auditors and audit firms with respect to the Chamber of Auditors - non-performance of internal regulations of the Chamber and tasks arising from their membership in the Chamber of Auditors = 6 auditors,

Article 37 par. 4 - non-payment of fees to the Chamber of Auditors and of other monetary payments = 3 auditors,
Articles 20 and 23 – audit documentation, auditor's report = 1 auditor.

Cases of breach of integrity of independent auditors and audit firms for 2010-2015 were not identified.

The principle of objectivity requires all auditors not to misuse their professional or business judgment due to bias, conflict of interest or unacceptable influence of other entities. It follows from the foregoing that an audit client cannot interfere with the performance of the audit or otherwise exercise unacceptable influence over the auditor. Under the Code, the auditor must be independent from the client. Independence under the Auditor's Code of Ethics is defined as:

a) Independence of the mind

- A state of mind that allows an auditor to express an opinion without being influenced by issues distorting professional judgment, thereby enabling an individual to act with integrity and apply objectivity and professional scepticism.

b) Independence of the conduct

- Avoiding facts and circumstances which are so significant that a reasonably thinking and informed third party, having considered all the specific circumstances and facts, is likely to conclude that the integrity, objectivity or professional scepticism of the firm or member of the audit team is distorted.

According to the Statutory Audit Act, the statutory auditor/audit firm is subject to inspection for the assurance of quality, which is performed by the inspectors of the Slovak Chamber of Auditors and to supervision by the Auditing Oversight Authority (hereinafter: the "UDVA") under Article 35 par. 4 of the Statutory Audit Act:

"The selection of entities to be subject to the statutory audit quality assurance review shall be made on the basis of an analysis of risks and shall be carried out at least every three years in the case of a statutory auditor and audit firm that carried out statutory audit of an accounting entity that is a public-interest entity, at least every six years in the case of other statutory auditors and audit firms."

Findings of tax authorities on double-entry accounting or other fraudulent accounting practices

Number of criminal complaints lodged with LEAs, reported harm, individual criminal offenses in 2011-2015:					
Complaint, harm, criminal offenses/year	2011	2012	2013	2014	2015
No. of complaints for suspected commission of tax crime, total	1862	842	1214	1118	485
Reported harm in ths. €	247 530	123 322	94 771	184 878	83 884
§ 278 - Failure to Pay Tax and Insurance	636	266	494	247	96
§ 277 - Failure to Pay Tax and Insurance, Tax fraud	315	183	270	312	154

§ 276 - Tax and Insurance Evasion	1043	475	532	579	313
§ 259 - Distortion of Data in Financial and Commercial Records	59	16	22	5	2

However, statistics from the Financial Administration do not include criminal proceedings for tax crime resulting from the development of the operational units of the Police Force and criminal proceedings initiated on the basis of cooperative coordination between FA, PF, ... and these are actually the largest criminal proceedings where they act against organized groups. In these cases, even the criminal complaint was not lodged many times.

Lodging a criminal complaint itself is only the first attempt for intervention by LEAs. But the efficiency reaches finally only about 5-6% - convicted persons for tax offenses based on complaints lodged by the Financial Administration.

h3) CDD framework quality

1. Availability of reliable identification infrastructure

The SR currently has a high-quality and secure identification system, as evidenced by a small number of detected falsified identification documents ("IDs"). Each type of identification document is governed by a separate law and relevant regulations, e.g., the Act on identity cards, the Act on Travel Documents, the Asylum Act, and the like. The IDs issued in the SR are continuously supplemented with each new series with additional security features and properties that complicate the possibility of their falsification.

Obliged entities in the Slovak Republic in connection with the ID of Slovak citizens use the verification service - a publicly accessible page of the Ministry of Interior of the Slovak Republic aimed at searching for lost and stolen documents, which is implemented by most banks in their verification systems. Some bank offices have a reading device that reads the numerical data on the back of the ID and can then evaluate it from the identification data of the control margin whether the document has not been altered.

On the basis of the information available, it can be concluded that statistics on individuals who do not have proper IDs and statistics on specific persons (immigrants, social groups, etc.) are not kept and such data would have a low explanatory power. The conditions for issuing documents for a group of immigrants are specifically regulated by the applicable law (Asylum Act).

A negative and growing trend can be noticed in the number of false travel documents of aliens identified in the Slovak Republic. Another vulnerability is the slightly increasing trend of using false identity - the use of genuine identification documents in connection with the false identity of an unknown person, with the use of the similar appearance of the person with the person in the photograph in the document, the so-called "look-a-like".

Statistics on the number of cases for the period of 2010 - 2015, where false identification documents of Slovak citizens were used (ID cards, passports, other identification documents of a citizen).

	2010	2011	2012	2013	2014	2015	TOTAL
Travel passport	10	9	23	1	1	0	56
Diplomatic passport	0	0	0	0	0	0	0
Service passport	0	0	0	0	0	0	0
Identification card	30	24	10	8	4	3	79
ID card	3	3	3	4	1	3	17
Driving license	37	36	17	18	9	3	120
Visa	0	0	0	1	0	0	1
Residence permit	0	0	2	0	0	0	2
Other	0	0	0	0	0	0	0

Statistics on the number of cases for the period of 2010 - 2015, in which genuine identification documents of Slovak citizens were used in connection with the false identity of another person (ID cards, passports, other identification documents of a citizen).

	2010	2011	2012	2013	2014	2015	TOTAL
Look-a-like	0	0	2	0	0	1	3
(misuse of the genuine document by another person)			(residence permit for stay in SVK)			(Identification card SVK)	

Statistics on the number of cases for the period of 2010 - 2015, in which false identification documents of foreign citizens were used in the Slovak territory (ID cards, passports, other identification documents of a foreign citizen).

	2010	2011	2012	2013	2014	2015	TOTAL
Travel passport	26	8	42	9	105	226	416

Diplomatic passport	0	0	0	0	0	1	1
Service passport	0	0	0	0	0	0	0
Identification card	33	17	18	8	9	22	107
ID card	0	0	0	0	0	1	1
Visa	1	7	18	5	11	9	51
Residence permit	10	22	89	10	3	2	136
Driving license	15	2	10	5	8	11	51
Other	0	0	3	1	0	0	4

The Institute of Forensic Science of the PF provided information on cases with false and altered documents for a period of 2010 –2015:

Year	ID cards SR		Foreign ID cards		Travel passports SR		Foreign travel passports	
	altered	false	altered	false	altered	false	altered	false
2011	11	22	0	2	10	0	3	0
2012	7	13	0	3	8	0	2	0
2013	3	18	0	1	10	1	1	0
2014	2	7	0	0	3	1	0	0
2015	2	6	0	0	2	0	0	0
Total								

Note: These figures refer to falsified and altered documents that were examined and kept on file by the Institute of Forensic Science PF in the relevant years.

2. Availability of independent information sources

On the basis of the information available and consultation with the representatives of the obliged entities, it can be stated that obliged entities use mainly the following independent sources of information and their own internal sources:

- Information from a credit register that is accessible to banks (most banks use this information in particular when assessing clients before applying for a loan, or refinancing credit or the occurrence of outstanding payments).
- Information from the Social Insurance Agency (which is used in particular when assessing clients applying for a loan; banks obtain information about the amount of the monthly salary of the client or information on the employer who pays compulsory payments for the employee),
- Information from the Land Registry,
- Internal client history information (account statements, past bank product applications, existing products provided, "black" and "grey" lists, questionnaires for bank products, KYC questionnaires prior to establishing a business relationship, and

- during a business relationship, etc.) - internal information,
- Some banks have their own internal systems into which they deposit preliminary information on specific transactions (when depositing cash in a larger volume, a note on origin of funds will be entered to the system if the client responded to the question of the bank's employee, etc.),
 - Information from freely available sources (social networks, Slovak Commercial Register, Trade Register of Slovak Republic, FOAT, information on economic results of business entities and companies, e.g., www.finstat.sk, etc).
 - IT tools for KYC: databases of ownership structures, databases of sanctioned persons, PEPs databases, systems for identifying social and economic links and relations, etc.

3. Availability and access to BO information

In the period under review (2011 - 2015), information on beneficial owners of legal entities (ultimate beneficial owners) was not kept in the SR in any central register. The obligation to identify information about the beneficial owners is imposed on the obliged entities under Act no. 297/2008 Coll. In carrying out customer due diligence, obliged entities are obliged under Article 10 par. 1 b) of Act no. 297/2008 Coll., with regard to the risk of legalization or terrorist financing, identify the beneficial owner and take adequate measures to verify his identification including measures to determine the ownership structure and management structure of a customer being a legal entity or a corporation. If the obliged entity cannot perform customer due diligence pursuant to Article 10 par. 1 a) - c) of Act No. 297/2008 Coll. due to reasons on the part of the client, (i.e. also if the client refuses to provide the obliged entity with information about beneficial owners), the obliged entity must refuse to enter into a business relationship, terminate a business relationship, or refuse to perform a particular business. The obligation to identify the beneficial owners is also imposed on corporations (foundations, non-profit organizations providing general public services, non-investment funds) in Article 25 of Act no. 297/2008 Coll. Corporations are required to keep a written list of beneficial owners that they are required to submit during an inspection by the FSJ.

In the SR, the first register of BOs for the purpose of enhancing the transparency in the disposal of public funds, only in 2015. Based on Act No. 252/2015 Coll., which supplemented and amended Act No. 25/2006 Coll. on Public Procurement and on Amendments to Certain Laws as amended (hereinafter "Act No. 252/2015 Coll."), the contracting authority was obliged to enter the beneficial owners into the Register of beneficial owners (hereinafter "BOR"), which was published on the website of the Public Procurement Office (hereinafter referred to as "PPO"). The BOR was developed as a public administration information system, the administrator of which became PPO and included data on the beneficial owners. BOR was publicly available. Legal or natural persons interested in participating in the procurement procedure were therefore required to register the beneficial owner into the BOR. In the BOR, lists of beneficial owners were registered stating the first name, surname, address and also data establishing the position of the beneficial owner, including data on whether the beneficial owner is a public official. On 1.2.2017, Act No. 315/2017 Coll. on the Register of Public Sector Partners and on amending and supplementing certain laws became effective. The BOR was replaced by a Register of Public Sector Partners (hereinafter "RPSP"). Unlike the BOR, RPSP covers not only relations arising from public procurement but its scope

covers a wide range of transactions between the state (or the public sector) and natural and legal persons not only through public procurement, but also, for example, the provision of funds from European funds, the provision of subsidies or other state aid, the conclusion of purchase, lease or other contracts, as well as the assignment of state receivables, etc. The Ministry of Justice of the Slovak Republic is the administrator and operator of the RPSP. The Registration authority (the authority performing data entries) is the District Court Žilina.

However, even after the development of the RPSP, Slovakia does not perform the obligation imposed on Member States by the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, which requires that Member States shall ensure that corporate and other legal entities incorporated within their territory are required to obtain and hold adequate, accurate and current information on their beneficial ownership, including the details of the beneficial interests held. Information on beneficial owners should be kept in the central register of beneficial owners, which should be created in the Register of Legal Entities, Entrepreneurs and Public Authorities (hereinafter: the Register of Legal Entities). The Register of Legal Entities was established on the basis of Act No. 272/2015 Coll. on the Register of Legal Entities, Entrepreneurs and Public Authorities, and on amending and supplementing certain laws, as amended, the purpose of which was to establish a Register of Legal Entities complying with the requirements of the National Concept of Informatization of Public Administration.

QUALITY OF CRIMINAL PROSECUTION OF FINANCIAL CRIME

The basic prerequisite for effective prosecution is the ability and integrity of law enforcement authorities to initiate and conduct criminal prosecution of the offenses of legalization of proceeds of crime. However, this must be preceded by effective detection of the legalization of proceeds of crime, the identification of proceeds and their movements, and the activities of the competent authorities in the field of operative searching activity and criminal intelligence.

a) Capacity and sources for criminal prosecution in the area of financial crime

a1) Police Force units

Investigators performing criminal investigation of the legalization of criminal proceeds and predicate offenses are included in the criminal police departments of the Police Force District Offices, the Regional Offices of the Police Force, the Criminal Office of Financial Administration, and the National Criminal Agency. Investigators gain experience in investigations of predictive offenses based on the number of years worked, but experience in the field of property seizure and financial investigation is inadequate, or none. At the end of the period under review, some attention started to be paid gradually to this area as a result of the measures taken for financial investigation.

Criminal offenses of economic nature are also investigated by the Criminal Police Department of the District Directorate of PF and the Criminal Police Department of the Regional Directorate of PF at the Economic Crime Units (units 2, 3 or 4). The burden at the

Economic Crime Units is higher than at the Property and Violent Crime Units. Within the organizational structure of NAKA, a National Financial Police Unit is established to detect and investigate the most serious forms of criminal offenses against property and criminal offenses of economic nature if such criminal offence causes damage or brings a benefit which is at least twenty-five thousand times higher than the amount of small damage set out in the Criminal Code, to which also the powers of the Specialised Criminal Court apply. At the same time, the activity of the said Unit is also suspected crimes showing elements of organized crime, with the identification of the participation of organized and criminal groups or the representation of persons from the environment of organized crime³¹.

Systematic training - police training in the field of legalization/property seizure did not exist in the period under review. The process was accelerated on the initiative of GPO SR in connection with financial investigation. NAKA subsequently organized one international seminar on the issue of Financial Investigation and Confiscation of Property for a narrow circle of participants only in October 2016. Seminars and training in the area of financial investigation conducted at the level of the Public Prosecutor's office for capacity reasons are logically not accessible to all police officers. The first official methodological guidelines for the financial investigation were adopted after the period under review.

a2) Public Prosecutor's office

Public Prosecutor's offices are adequately structured, funded and staffed by persons with appropriate training and skills. The Special Prosecutor's Office (USP) of the General Prosecutor's Office of the Slovak Republic has a special position, which has the local and subject-matter jurisdiction for the supervision of prosecution of the most serious economic, organized crime solely in the field of corruption and terrorism, including the financing of terrorism. There is special training in the form of seminars, consultations and training organized under the Plan of Education of Prosecutors and Public Prosecutor's Offices Staff, which is adopted at the GPO SR level and mandatory for all levels of the Prosecutor's Office, as well as training plans adopted by the Regional Prosecutor's Offices, as well as for prosecutors specialized in criminal offenses against property and tax offense.

The criminal offence of the legalization of proceeds of crime often involves transfer of funds from foreign accounts, and legalization is derived, as a rule, only from the fact that it is suspicious payment based on additional notification of the sending foreign bank, whereas it is usually difficult to determine the real identity of the person who made the payment abroad or opened the account in this country. Often, they are people with a false identity or aliens. The investigation is made difficult and extended due to the execution of legal aid operations, often also in several countries, sometimes outside the European Union.

It can be noted that this is a latent, highly sophisticated crime, the identification and detection of which is primarily the responsibility of the intelligence and operational police authorities. The Public Prosecutor's Office can act actively and effectively influence the process only when the initiation of formal prosecution can be considered.

³¹ Most frequently, there are cases of carousel tax fraud, sham intra-Community supplies of goods, tax fraud on import and export of goods from third countries, cases of fraud and evasion related to invoicing and bookkeeping, as well as cases of illegal financial operations, illegal operations in the area of capital and financial markets, as well as cases of forgery, fraudulent alteration and illicit manufacturing of money and securities, etc.

In the case of the prosecution of a criminal offense of sharing, the prosecution often takes place on the basis of internal knowledge of the law enforcement authorities, but it is problematic to prove that the suspected person (participant) knew the origin of the thing, i.e. that it originated from criminal activity. Most things come from theft when perpetrators of the original offenses sell the objects for a fraction of the market price in order to get money for their personal consumption. For the deliberate form of this offense, the demonstration of fault in many cases depends on the testimony of the potential perpetrator (participant) and the testimony of the perpetrator of the crime who obtained the object that was to be subject to the sharing crime. For the negligent form of sharing, it is also problematic to prove the subjective aspect of the crime (perpetrator often does not know that the object comes from crime, although he should and could have known it, or he reasonably relied, that it was not an object from criminal activity).

Serious ways of the legalization of proceeds of crime are linked to the most serious forms of crime committed by various sophisticated ways, where detection, evidence and the actual investigation of the so-called predictive offenses are both time consuming and demanding in content. In such cases, LEAs have only limited personal and technical capabilities to prove in parallel the so-called predictive offense and the way of legalization of proceeds of crime. In the period under review, sufficient conditions were not created for the identification of the proceeds of crime through a sufficiently efficient system of proactive and parallel financial investigation. The said processes contain the necessary requirement of multi-sectoral specialization. Plus, without effective seizure of property in the early stages of criminal proceedings, the basic conditions for the successful withdrawal of the proceeds of crime will not be created. It will therefore be necessary to streamline the concepts of seizure - criminal prosecution for several criminal cases is delayed and the perpetrators do not have any assets or funds at the time of the prosecution that could be seized (at the time of indictment, the property was transferred to other persons a long time ago).

A particular aspect that adversely affects the operation of LEAs was the absence of efficient information systems for managing files and documents and then obtaining relevant statistical data. From the point of view of the horizontal approach to effective verification and detection of crime, the absence of links between current police, prosecution and court systems is also a negative fact. The current state virtually did not allow "to track" a specific case from the initiation of the criminal prosecution to the final court decision. There is no statistics on the number of investigators involved in the property seizure process.

b) Integrity and independence of LEAs in the area of financial crime

b1) Police Force units

Investigation is conducted without interference, political or social pressure, corruption, intimidation or abuse of the position, as well as property seizure is executed without undue external intervention. The investigator is independent in the process. Supervision of the lawfulness under the Criminal Procedure Code is carried out only by the prosecutor.

Number of cases of misuse of office by a public office-holder committed by police officers in the crime investigation or clarification activities	2011	2012	2013	2014	2015
	5	7	15	2	2

In the period between 2011 and 2015, no cases of the misuse of office by a public office-holder were reported in the investigation of the offences of legalization of proceeds of crime or sharing. Also, no cases of the interference with political or social pressure, intimidation, etc., which had an impact on the results of the investigation, were reported.

Statistics relating to the criminal activity of Police Force members who have been charged with the legalization of proceeds of crime under § 233 of the Criminal Act.

Number of accused police officers - offence under § 233 Cr.A.	2011	2012	213	2014	2015
	1	1	3	1	2

b2) Public Prosecutor's office of the SR

The execution of prosecutors activities in the area of financial crime is not specifically regulated. Independence of prosecutors is generally ensured by law (Act No. 154/2001 Coll. on Prosecutors and Candidate Prosecutors, as amended). The constitutional position of the Public Prosecutor's Office as an independent body ensures that prosecutors who cannot be members of any political party, work without political influence and are appointed to their function in a lifetime. They conduct supervision of the observance of lawfulness in the pre-trial procedure by law in every criminal case where criminal prosecution is initiated, as well as before the prosecution is initiated.

The Prosecutor has the statutory right to act as a prosecutor without intimidation, duress, impediments, inappropriate interference or unauthorized exposure to interference with his powers and personal responsibility.

The superior Prosecutor is entitled to issue a (written) instruction to the subordinate prosecutor on how to proceed or decide that another subordinate prosecutor will execute it. This power is not absolute. In principle, the Prosecutor has the right to ask the superior Prosecutor for the withdrawal of the assigned case if he considers the superior Prosecutor's instruction to be inconsistent with the law or with his legal opinion. The superior Prosecutor shall satisfy his request, and shall delegate another Prosecutor to address the case, or will do it himself. In proceedings before a court, the subordinate prosecutor is not bound by the instruction of the superior Prosecutor, if in the course of the proceedings any change in evidence occurs. A subordinate prosecutor is obliged to refuse to comply with the instruction if he would commit a criminal offense, misdemeanour, other tort, or disciplinary offense; the refusal to fulfil the instruction must be in writing. A subordinate prosecutor may also refuse to comply with the instruction if due to such performance he directly and seriously endangers his life or health or directly and seriously endangers the life or health of his close person, and if the subordinate prosecutor assumes that compliance with the

instruction might result in the occurrence of damage, he is obliged to notify the superior prosecutor.

The so-called negative instructions are legally limited. The superior Prosecutor cannot issue an instruction to the subordinate prosecutor not to initiate criminal prosecution, not to bring an indictment, not to file a motion to remand an accused person in custody, to refer the case to another authority, to stop the prosecution of another authority, stop the prosecution, to bring an indictment or to apply for a regular or extraordinary remedy to the detriment of the accused, also to commence proceedings before the court, not to enter the court proceedings, not to file an appeal against a court decision under special regulations, not to file protest of the prosecutor or not to file a warning of the prosecutor.

The basic duties of the Prosecutor include the obligation not to be affected by individual or partial interests, the interests of political parties or political movements, not to succumb to pressure of the public opinion or the means of communication, and to refuse any interference, pressure, influence or request that could threaten his impartiality while acting objectively and considering all decisive circumstances, regardless of whether they are beneficial or not beneficial for the participants in proceedings, and to protect human dignity, fundamental human rights and freedoms, not to disadvantage or prejudice the parties or participants in proceedings on grounds of their gender, race, skin colour, language, belief and religion, political or other opinion, national or social origin, nationality or ethnic group, property, birth or other status.

The Prosecutor is disciplinary responsible for the culpable non-performance or breach of the prosecutor's duty, the prosecutor's conduct, which raises reasonable doubts about his conscientiousness and impartiality in the decision-making process, the prosecutor's conduct in public, which downgrades the seriousness of the public prosecution.

The Prosecutor Self-Management Bodies - the Regional Prosecutor's Assembly and Regional Prosecutor's Councils are set up to ensure the provision and protection of the rights and legitimate interests of prosecutors. The Prosecutors' Council is the supreme executive body of the Prosecutors Self-Government with national powers, whose role is also to coordinate the activity of Prosecutors Councils. Self-Management Bodies have statutory decision-making, approval, amendment and advisory powers. Rules of Prosecutor's Ethics are contained in the Prosecutor's Code of Ethics. The Prosecutor's Code of Ethics is approved by the Prosecutor's Council and published on the General Prosecutor's Office website.

An evaluation of the data from the Register of Seized Things in relation to the issue of conflict of interest with the eventual adoption of appropriate measures shows that in the evaluation period it was decided to exclude the prosecutor from the execution of criminal proceedings only in two cases.

c) Efficiency of national cooperation

Based on requests for cooperation, national cooperation is at the required level. Cooperation between the police and the prosecution units has long been developed at both central and local levels. In specific cases there are no formal barriers to effective

communication between acting police officers and prosecutors. Room for improvement is in the speed of handling requests, which is, however, affected by the current burden of the requesting unit. Cooperative meetings at all levels of police and prosecution authorities, including AML/CTF issues, are an immanent component of cooperation.

d) Efficiency of international cooperation

Judicial cooperation

Slovakia has a sufficient legal framework for providing and requesting legal assistance from abroad. The apparent shortcoming is only the length of time for handling requests from foreign state authorities. The SR provides legal assistance as soon as possible. Cooperation in the field of legal assistance in criminal cases is de facto covered by the GPO SR, which coordinates and supervises the proper and timely handling of requests.

Supervision over the fast provision of legal assistance requests, the handling of which is to be provided by the investigator, is carried out by a prosecutor who, if necessary, effectively coordinates the work of the investigator so that it is handled properly and timely. The SR is able to provide legal assistance on request for cooperation carried out on the basis of proceedings without prior conviction and related preliminary rulings.

Slovak provides urgent legal assistance on request, and legal assistance is also provided regardless of whether the perpetrator has been convicted of an offense abroad or not. Restrictions on the provision of information are appropriate to the circumstances and areas from which the information is required. Information is provided bilaterally in accordance with law.

Investigators consider legal assistance from some countries to be lengthy. The most problematic cooperation has been identified from Canada, the USA, China, United Kingdom, Italy, and France. The quality and timeliness of cooperation with Asia and Africa have been assessed by the investigators as very weak.

QUALITY OFFG JUDGMENTS

The basic prerequisite for effective criminal justice is competent and incorrupt judges who conduct criminal proceedings professionally and correctly.

e) Capacity and resources for judicial proceedings³²

A large number of court officials takes the view that the capacity and resources for criminal prosecution in financial crime are inadequate. For this reason, it would be necessary to plan the specialization of judges in the decision-making process of financial crime in the framework of the decision-making powers of court. This would, however, mean the need for

³² Despite the efforts of the NRA Coordination Body, it was not possible to ensure the direct participation of judges in the work of teams to assess the overall level of threats and vulnerabilities of legalization at national level. The information relating to the legal proceedings was thus obtained through other persons, from the representatives of the MoJ SR.

the reinforcement of staffing of the court, given that type kind of crime, with respect to its gravity and complexity, would require more time to study and prepare the hearing but also the decision itself, and thus the judge would be able to decide on less cases than in the case of „general crime.“ One of the courts, on the other hand, states that courts have adequate professional, organizational and material means for effective prosecution of perpetrators, but recommends that the thematic training in the financial sector - banking, as it is a specialized issue, should be included in their education. However, another court considers that although the Judicial Academy organizes seminars for judges, these are not mandatory, and it is up to each judge to attend or not to attend the seminar.

Also, it should be noted that the legalization of proceeds of crime is within the competence of the Specialized criminal court if such crime caused damage or gained profits of at least twenty-five times the amount of minor damage under the Criminal Code, or if such criminal offence caused damage or brought a benefit which is at least twenty-five thousand times higher than the amount of small damage set out in the Criminal Code or if such criminal offence was committed in the scope that reaches an amount of at least twenty-five times the amount of minor damage under the Criminal Code.

In the field of education, the concept of education of judges should be based on the intention to acquire and get deeper knowledge of the financial market, securities, capital market, insurance, tax, but also accounting or banking, and the study should (at least four semesters) be organized in a longer period of time, and the education should guarantee an increase in professional knowledge and thus the ability and skills of judges for legal issues related to the economic issues covered by the relevant study plans of judges. The court in question thinks that the judges would acquire skills after completing this form of education, which would also facilitate their communication with forensic experts and at the same time they would be able to better orientate in expert opinions prepared in connection with criminal proceedings on property and economic criminal offenses.

Insufficient training and specialization of judges in AML/CTF issues can be seen as vulnerability.

b) Integrity and independence of judges

The independence of judiciary bodies and the independence of the courts are therefore connected with the performance of duties entrusted to them by the Constitution.

Independence with the impartiality and expertise (qualification) of a judge is a prerequisite for quality decision-making and predictability, and thus the importance of the proper performance (provision) of justice. Independence and impartiality are closely related, often overlapping and not always easy to distinguish from each other. Impartiality defined also as an absence of prejudice (bias) and partiality is used to be considered a term wider than independence. The impartiality of a judge must be the essence of his function, while his independence should only make it possible. Judicial independence and impartiality must also be understood as the independence and impartiality of each individual judge (*Resolution of the Supreme Court of the Slovak Republic of 23 May 2012, file ref. 1 Nc 30/2012*).

The independence of a judge must also be seen as independence from the components of the political system, and also as independence within the judiciary power itself (the entire judicial system and the particular court in which the judge works); it is also independence from public opinion or means of communication. Only such an understanding of independence is a prerequisite for the impartiality of a judge that no one can threaten.

As for independence, one of the courts says that doubts about the independence of the judiciary bodies in our conditions may induce the influence of the Bar Association in situations where its representatives are members of the selection boards for the position of judges, they are members of the Disciplinary boards panels making decisions on judges and are also members of the Judicial Council of the Slovak Republic. The court further states that it cannot be ruled out without any doubt that such persons defend or have previously defended persons prosecuted for ML offenses. The court is of the opinion that another danger that may jeopardize the independence of the judiciary bodies is the increasing influence of NGOs on legislation, in situations where their sources of funds are not transparent.

The Judicial Council and the self-management judicial authorities have a major influence on decision-making on the appointment of judges and their career, represent an appropriate way of guaranteeing the independence of the judiciary bodies, and judiciary bodies as such are in line with international standards. Despite that, media and NGO representatives during the GRECO evaluation visit expressed serious concerns over the improper political influence that the executive power representatives exercise in the Judicial Council (but also in the Disciplinary boards panels and the Selection Committee) from the position of their political membership.

Also, we can note with regret that the SR remains one of the EU Member States with the worst perceived independence of the judiciary bodies. This is regularly highlighted by the material published by the European Commission in an EU justice comparative report assessing the quality and independence of judicial systems in the EU Member States. The comparative report provides data on the perceived independence of the judicial system based on the annual Global Competitiveness Report of the World Economic Forum.

The quality of ML judgments is directly dependent on the nature and complexity of individual criminal cases. In this area, there is a relatively well established practice of the courts on the evidence of the origin of the proceeds of crime. Relatively high demands are still being placed on the standard of evidence when demonstrating the subjective aspect of the legalization moment. In both cases, as regards the demonstration of facts based on indirect evidence derived from objective and factual circumstances. A particular challenge is the established practice of the courts in the area of seizure of the proceeds of crime. The practice in the area of decisions on the application of the compulsory forfeiture of assets still can be marked as not well established.

Another element that affects the effectiveness of criminal prosecution is the length of the entire criminal prosecution process, especially court proceedings. Based on the available statistics from the courts of the SR as well as the statistics obtained from a study prepared by the European Commission entitled EU Justice Scoreboard 2017, which contains statistics

on criminal offenses for the years 2014 and 2015 regarding legalization, it can be stated that the length of the proceedings in 2014 was approximately 300 days, whereas it fell below 200 days in 2015. However, in qualitative terms, these statistical data must be considered insufficient as they are de facto a mathematical average and do not reflect the time-consuming nature and length of court proceedings in national cases of criminal offenses of economic nature and the like (according to empirically verifiable facts, court proceedings of length of 5, 6, 7 or even more years are not exceptions). For this reason, despite the statistical downward trend, the length of proceedings, including the preparatory procedure, may have an impact on the overall vulnerability of the system, and it is necessary to develop activities that will help to increase the effectiveness of criminal proceedings in order to shorten their overall length without affecting their final outcomes.

Special assessment of the impact of the concept of statutory bar

The limitation periods for the statutory bar on prosecution and statutory bar on the execution of punishment are laid down by the Criminal Act, which are primarily based on the seriousness of the offense and are sufficient in the case of the offences of sharing and the legalization of the proceeds of crime. There were no cases of criminal prosecution in the area that would have to be discontinued for the said reason. The suspension of the limitation period, i.e. that it does not lapse for legally defined statutory reasons, and the interruption of the limitation period also contribute to the fact that the statutory bar does not have a significant impact on vulnerability.

QUALITY OF A FRAMEWORK FOR SEIZURE OF PROPERTY AND WITHDRAWAL OF PROCEEDS OF CRIME

In the period under review, effective legislation made it possible to seize income and proceeds derived from criminal activity, profits derived from these crimes and property of the relevant value, to a considerable extent but to a limited extent. Application problems were identified, in particular, in the area of seizure of property acquired for criminal proceeds received by another person, as well as under certain conditions in the area of the application of the concept of seizure available to ensure the execution of property punishment, e.g., demonstrating a reasonable concern that the execution of this punishment will be frustrated or made difficult. The issue of substitute value also appeared problematic. Practically, it was difficult to seize the property of third parties. It was not possible to seize third party's property, except for the property of the perpetrator that was mixed with the third party's property. It is possible to seize the thing of a third party for the purposes of executing the confiscation of a thing (§ 461 CCP), since a judgment imposing protective measure for the confiscation of a thing can also be made which, as a sanction, may affect the property of both the third party and the perpetrator. Operational police officers in fact did not have any means for the seizure of the proceeds of crime under the Act on Police Force. Legislation did not allow sufficient seizure of property and a thing on the ground that in some cases it links it up to the defendant's procedural position, so the current regulations on

the seizure of property and things cannot be considered as allowing a sufficiently efficient procedure in all cases.

Systematic training in how to monitor the flow of proceeds of crime has not been attended by the investigators yet. Investigators have sufficient technical resources to carry out "routine" tasks. In case an unusual thing should be seized in criminal proceedings (e.g., large quantities of oil, scrap, grain, etc.), the investigator has serious problems with the seizure of the thing. In this case, it is necessary to seize the thing through the support centre, where there has been a case where the support centre stated that there is not enough funding for the transport and storage of the material and for that reason it was impossible to seize the thing. In the context of property seizure, the problem is also the missing entity, which would manage all the seized property (and the execution of property-related decisions) in a comprehensive manner. The Prosecutor-General in the Report on the Prosecutor's Office Activity 2015 clearly points to the absence of an office for the management of seized proceeds and things from crime and an office for the return of seized proceeds and things to legitimate owners and the injured persons (AMO). This management is de facto left to LEAs, which does not allow the proper management of seized things (both movable and immovable), as a result of which their impairment occurs. The administration of property that cannot be secured by the Police Force is carried out by legal entities or public authorities.

Under § 3 of the Code of Criminal Procedure, property may be searched for, based on which a police officer may ask public authorities, higher territorial units, municipalities and other legal entities and natural persons to provide information on the property and income of persons. The search for property and income is also possible through operative-investigation and intelligence activity. Property search is also performed by lustrations in the records, which are available to the Police Force members (Mol, informative extract from the real estate register). For the seizure of property, the SR has, in principle, the necessary legal options, although there are some shortcomings. In some cases, seizure is possible only from the accused, that is, after bringing an indictment. Seizure of property as a whole is only possible from the accused.

Under Article 26 of Act No. 91/2016 Coll. on Criminal Liability of Legal Entities, limitation and seizure measures may be imposed on legal entities. The Code of Criminal Procedure provide a wide range of property seizure tools, but application issues are linked to some seizure options. Legislation provides protection of rights of third parties acquired in good faith.

It is not possible to seize the property of third parties except the property of the offender mixed with the third party's property. Also, no substitute value can be seized. The deficiency is that information obtained by PF units under regulations other than the Code of Criminal Procedure must be re-requested by the investigator under the Code of Criminal Procedure.

A great problem is the absence of a central bank account and the impossibility to conduct online bank account tracking. The ability to track property is totally absent, it is only possible to determine the status by sending requests to the relevant institutions, whereas it is not active property tracking in real time.

To ensure the claim of an injured party under § 50 CCP requires the demonstration of reasonable grounds to believe that the satisfaction of the injured party's claim for damages will be obstructed or made impossible, which must be omitted, as long as LEAs may demonstrate reasonable concerns that the transfer of property occurs, which makes the application of this provision impossible. Also, in this provision it is necessary to modify the term damage, since in the case of tax offenses it is not possible to use the provision in question on the grounds that its scope is determined for tax offenses and does not constitute damage within the meaning of the CCP. Based on the information available, this provision is little used. Another problem is the proof that the property acquired by the perpetrator was at least to a large extent acquired in relation to criminal activity or from proceeds of crime (§58 par. 2 CCP). The biggest problem with respect to the seizure of property is the absence of element managing all seized property.

Execution of the judgment of forfeiture of property

The provision of § 425 CCP governing the execution of the judgment of forfeiture of property⁸ or the provision of § 428 TP CCP governing the execution of the judgment of forfeiture of a thing⁹ stipulate, as one of the preconditions for the application of the said provisions, the necessity of the existence of concerns, „*that the execution of the punishment will be frustrated or made difficult.*“

However, this requirement has proved to be hardly demonstrable in practice. If the condition is kept, the vulnerability could be identified in view of the difficulty in proving it, but after identifying the problem, it was proposed that the legislator remove the mandatory condition from the cited provisions. An amendment to the criminal codes is planned in December 2017. § 425 CCP governing the execution of the judgment of forfeiture of property and § 428 TP governing the execution of the judgment of forfeiture of a thing will be amended and the mandatory condition of the existence of concerns that the execution of

⁸ The wording of § 425 par. 1 CCP is as follows: "*If the accused is prosecuted for an offense for which in respect of the nature and gravity of the act and the situation of the accused the imposition of the forfeiture of property can be expected, and there are concerns that the execution of this punishment will be frustrated or made difficult, the court and Prosecutor may seize the property of the accused in pre-trial proceedings. The court will always seize the property of the accused if it imposed a punishment for property forfeiture by a judgment which has not yet entered into force. In the seizure of the property of the accused the court proceeds accordingly based on [§ 50 par. 2 and 3](#), [§ 94 - 96](#). Upon the declaration of bankruptcy, the procedure for the punishment of the forfeiture of property is governed by a special regulation regulating insolvency proceedings; upon the takeover of property by the insolvency administrator, the seizure ceases to exist.*"

⁹ The wording of 428 par. 2 CCP: „*If the accused is prosecuted for an offense for which in respect of the nature and gravity of the act and the situation of the accused the imposition of the forfeiture of a thing can be expected, and there are concerns that the execution of this punishment will be frustrated or made difficult, the court and Prosecutor may seize the thing of the accused in pre-trial proceedings. The seizure shall be governed by § 50 par. 2 and 3, § 94 - 96 and § 425 par. 2 accordingly.*“

the punishment will be frustrated or made difficult, resulting from the provisions, will be deleted.

In the field of proof of origin of assets, in 2015, 52 cases were recorded where the proceeds, property value and method of their acquisition were examined. 37 cases were terminated out of the total number of 52 cases. Out of the 37 terminated cases, in 17 cases, the determined property was lower than 1500 times the minimum wage, in nine cases the identity of the notifier was not confirmed or the notification was incomplete and in 11 cases an initiative was sent to the prosecutor to file a motion to initiate proceedings to declare that the property was at least 1500 times the minimum wage higher than the proven income according to the provisions of § 6 par. 1 of Act No. 101/2010 on proving the origin of property. No judicial proceedings have been conducted since the effectiveness of this Act, based on which illegally acquired property would be forfeited to the state. A shortcoming of Act No. 101/2010 Coll. on proving the origin of property is that the investigated person may just dispose of a part of property exceeding 1500 times the minimum wage at any time after the commencement of investigation, and the results of the work of the Financial Police to identify the property will become devoid of purpose and the objectives of the Act will not be attained. The period of determination of the decisive period for which the acquired property is to be examined is also problematic because the law does not determine this period at all, and therefore its determination is based only on the consideration of the acting bodies (which would be indefensible before the court).

The legislation **lacks an effective regulation of the investigation** of the financial situation of the perpetrator of crime, which results in a **low rate of utilization and the effectiveness** of the imposition of these penalties, or the use of procedural concepts of seizure (*Seizure of injured party's claim - § 50 Code of Criminal Procedure, Seizure of funds - § 95 TP, Seizure of book entry securities - § 96 CCP, Execution of the judgment of forfeiture of property - § 425 CCP, Seizure of a thing - § 428 par. 2 CCP, Seizure of property (in legal relationship with foreign countries) - § 551 CCP*).

The general obligation expressed in § 119 par. 1 d) Code of Criminal Procedure, according to which in the criminal proceedings the **personal situation** of the perpetrator must be **demonstrated** to the extent necessary to determine the type and size of the sentence and the imposition of a protective measure and other decisions appear to be insufficient to the submitters with respect to the need to properly and timely investigate the property of the perpetrator. This applies in particular to perpetrators of **serious criminal offenses against property and criminal offenses of economic nature** in which the professional and time-consuming investigation of the circumstances of the act often prevents a parallel and timely investigation of the property of the perpetrator, which in itself represents an expert and time-consuming process. This means that LEAs use the relevant process concepts to a limited extent to seize the perpetrator's property because they **do not have its actual inventory**, allowing the perpetrators of these crimes to **successfully dispose of the property in order to avoid the risk of assets being forfeited** in the event of conviction or the duty to compensate the damage (in particular, they use **fictitious transfers to third parties, charging property with third-party rights - pledges, execution based on fictitious claims, etc.**).

A timely and complete inventory of perpetrator's property executed at the initial stage of the investigation will lead to more frequent and more efficient use of the concepts of seizure and consequently to more effective punishment of offenders. Some legal consequences could be linked to the inventory itself with respect to the ability of the perpetrator to effectively dispose of the property such as the ineffectiveness of legal acts (particularly in relation to the disposal of property in relation to related persons) enforced either directly by law or by concept on a general basis of the objectivity of legal acts governed by general private law.

The absence of a targeted policy for proactive financial investigation and its practical implementation is a key factor in low efficiency rates in the period under review.

ASSESSMENT OF VULNERABILITY IN CONNECTION WITH CORPORATIONS ACTIVITIES

According to Article 9 e) of the AML/CTF Act, corporations means a) foundations, b) non-profit organization providing generally useful services, c) non-investment funds and d) other special-purpose corporations irrespective of its legal personality which manage and distribute funds. The purpose of corporations is to provide generally useful services.

Information on corporations is provided in the central registers of the Ministry of the Interior and is available on the Internet. The data in the central registers include: name, seat, Reg. No., names and addresses of the founders, purpose of the corporation. Information on corporations is provided also in the Register of Legal Entities, Entrepreneurs and Public Authorities (Act No. 272/2015 Coll. on the Register of Legal Entities, Entrepreneurs and Public Authorities, and on amending and supplementing certain laws). On 1 November 2015, the **Register and Identifier of Legal Entities, Entrepreneurs and Public Authorities (RPO)**, according to the applicable legislation, became the source of legally valid data. It is a single source of basic data on all legal entities (legal entities, entrepreneurs, public authorities) that are currently registered or recorded in more than 70 source registers and records through different information systems. The RPO was created in accordance with the National Concept of Informatization of the Public Administration and is part the e-government.

Year	Foundation		Non-profit organization		Non-investment fund	
	Registered	Deleted	Registered	Deleted	Registered	Deleted
2011	900	13	2 502	39	678	8
2012	930	7	2 688	38	690	11
2013	950	11	2 852	28	710	5
2014	980	8	3 033	34	722	9
2015	1003	8	3 306	29	733	13

AML/CTF control:

According to Act No. 297/2008 Coll., the FSJ is authorized to exercise control in corporations for the purpose of identifying the beneficial owner and verifying the veracity and correctness of data listed in the list of beneficial owners and for the purpose of checking disposal of property. During such a control the corporation shall have the same obligations as the obliged entity under Article 30 of Act No. 297/2008 Coll.

In the period under review, from 2011 to 2015, the FSJ carried out four controls in corporations, on the basis of which no violation of the obligations imposed on the corporations by Act No. 297/2008 Coll., was found.

General supervision:

The Ministry of the Interior acts in the section of foundations as a public administration body. With regard to the scope of its rights and obligations, it imposed the following fines for not submitting the annual report on foundations:

Year	Number of fines imposed	Total amount of fines (EUR)
2011	39	18,205,-
2012	42	19,860,-
2013	62	26,822,-
2014	92	38,356,-
2015	57	24,895,-

Summary of the number of court applications submitted by the Ministry of Interior due to the failure to submit the annual report even during the additional period:

Year	Number of applications submitted
2011	8
2012	14
2013	19
2014	17

In the period under review, from 2011 to 2015, no cases were ascertained when corporations would be used or misused for the legalization or terrorist financing. Since information from abroad points to the risk of corporations in the legalization of proceeds

and possible support for terrorist financing, the risks associated with corporations need to be assessed.

Vulnerabilities for corporations:

- Insufficient supervision of corporations - small number of controls, on the FSJ Control Dpt. is entitled to execute control for the performance of obligations imposed on the corporations in Act no. 297/2008 Coll. (the obligation to identify beneficial owners and the obligation to dispose of property in corporations in accordance with the purpose for which the corporation was founded),
- In the period of 2011 – 2015, according to Act No. 297/2008 Coll., corporations were not obliged to identify their donors and the persons to whom they had granted funds,
- Insufficient awareness within corporations of the protection of this sector from its misuse for TF.

DETERMINATION OF PRIORITIES BASED ON NATIONAL VULNERABILITY ASSESSMENT

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of public authorities and institutions. The priority was determined on the basis of an assessment of the impact of identified shortcomings on the activities of these entities as well as on the national AML/CTF system as a whole, in particular for its importance, nature and type of measures implemented.

2. Level of priorities:

- Quality of the information acquisition and processing by the FSJ and the conceptual activity of the authorities responsible for the detection and prosecution of financial crime
- Capacities and resources for detection of financial crime and identification of proceeds of crime
- Capacities and resources for criminal prosecution of financial crime
- Internal integrity and independence of bodies responsible for detection
- Complexity of the legislation on the seizure of proceeds and the forfeiture of property, including the execution of property-related decisions

2. Level of priorities:

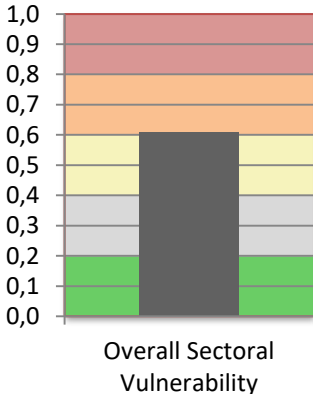
- Effectiveness of tax collection
- Quality of AML policies and strategies
- Availability and access to BO information
- Effectiveness of cooperation at national level in the field of AML

3. Level of priorities:

- Effectiveness of the legal definition of ML
- Capacities and resources for the judicial process
- Internal integrity and independence of the authorities responsible for the prosecution of judges
- Availability of reliable identification infrastructure
- Availability of independent information sources

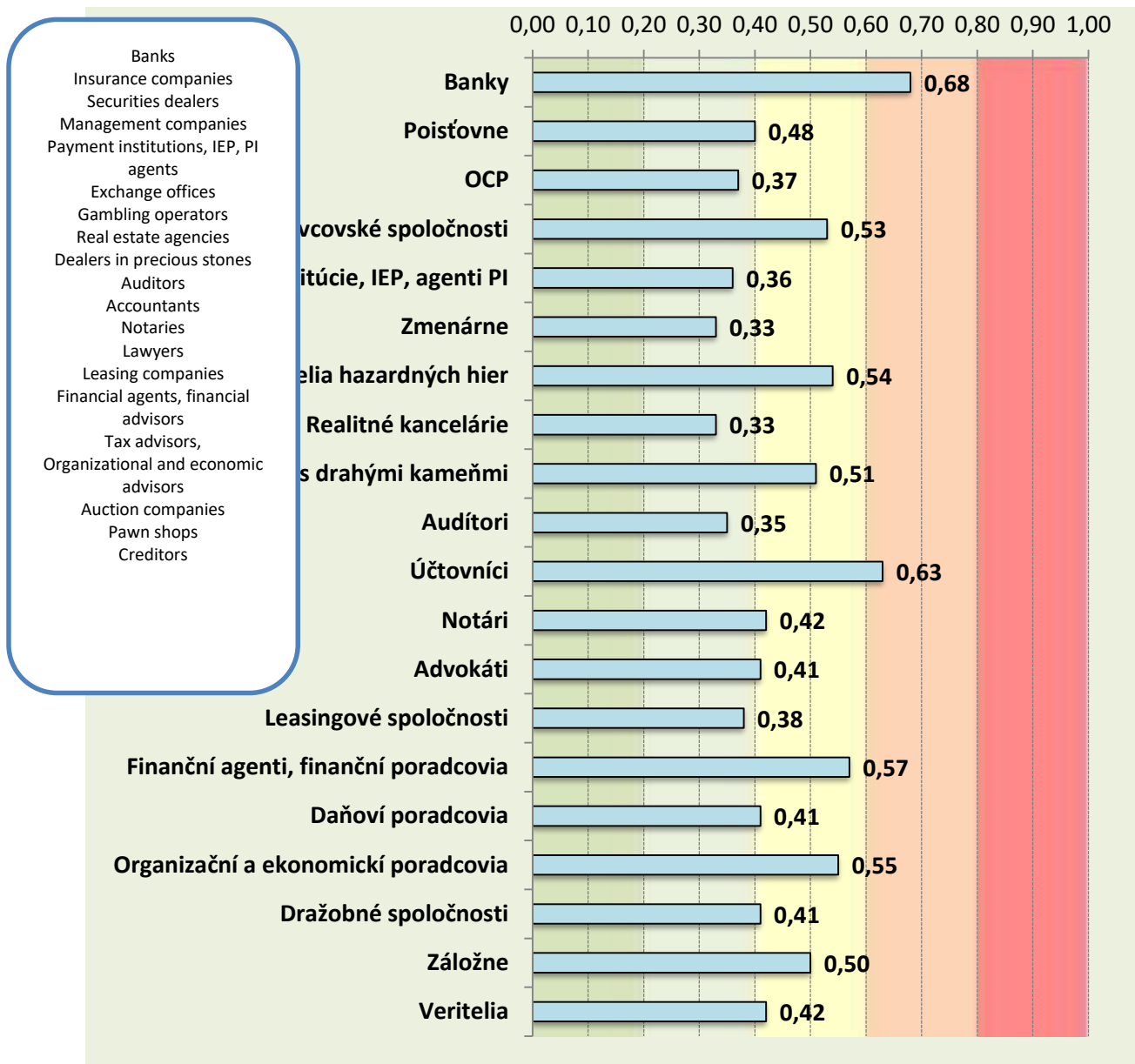
1.2.2 GENERAL EVALUATION OF THE OVERALL LEVEL OF VULNERABILITY OF THE SECTORS OF NATIONAL ECONOMY

The overall vulnerability of the sectors was assessed as **medium-high (the score according to the programme tool: 0,61)**. For an assessment of overall vulnerability of the sectors, vulnerability assessments determined by working groups for the following sectors: banks, insurance companies, securities dealers, management companies, payment institutions (together with electronic money institutions and payment institution agents), exchange offices, gambling operators, real estate agencies, dealers in precious stones, auditors, accountants, notaries, lawyers, leasing companies, financial agents and financial advisers, tax advisors, creditors, legal persons or natural persons authorized to execute auctions outside execution, legal and natural persons authorized to operate a pawnshop and legal and natural persons authorized to provide organizational and economic advisory, were used.



Among these sectors, the **medium-high vulnerability** in the prevention of legalization of proceeds of crime was evaluated in the banking sector (score 0.68) and the sector accountants (score: 0.63).

Medium vulnerability was evaluated for financial agents and financial advisers (score: 0.57), for legal and natural persons authorized to provide organizational and economic advisory (score: 0.55), for gambling operators (score: 0.54), for management companies (score: 0.53) – please see the graph below



Based on the generalization of the results of the evaluation gained, it is possible to identify the following **common factors**, which significantly affect the vulnerability in several evaluated sectors:

- Lack of awareness of obliged entities of the ML/TF risk and their management,
- Incompliance with otherwise adequate legislation,
- Insufficient number of controls carried out with obliged entities and corporations by AML/CTF regulators,
- Insufficient methodical and training activities by regulators,
- Absence of a central bank account record.

A specific factor of vulnerability within individual sectors of the national economy identified by the working group within the NRA was the establishment of a business relationship (relationships) without the physical presence of the client with a view to identifying and

verifying the identification (online identification via various mobile applications or other digital means). Vulnerability determinants:

- Possibility of using a false identity document or data coming from identity theft,
- Impossibility of assessing the holographic, security features of the identity document as well as the signs of unauthorized intervention with or the damage to the document,
- Possibility of modifying the client's face,
- Possibility of misusing a third person (a straw man) to establish a business relationship,
- Possibility of misuse of personal data on the Internet,
- Impossibility of assessing the environment outside of the camera image,
- Impossibility of implementing CDD measures according to the AML/CTF Act³³.

The detailed results of the evaluation of the various sectors of the national economy are presented in the following chapters.

DETERMINATION OF PRIORITIES FROM SECTORAL POINT OF VIEW:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of authorities in the area of AML/CTF supervision and control. The priority was determined by assessing the impact of identified shortcomings on the size and importance of the sector from the perspective of the national economy as well as with regard to the products and services provided.

Priority level	Area
1.	Banks
2.	Gambling operators
3.	Financial agents, financial advisors
4.	Management companies
5.	Accountants
6.	Dealers in Precious Metals and Stones
7.	Organizational and economic advisors
8.	Insurance companies

³³ According to the above stated, obliged entities will consider business relations without direct contact with the client (without using certain security measures such as electronic signature and official identifier) as a high risk factor and they will take this into account when assessing the risks under the AML/CTF Act and in such cases they will perform enhanced CDD.

9.	Tax advisors
10.	Financial leasing
11.	Creditor
12.	Lawyer
13.	Pawnshops
14.	Payment institutions, electronic money institutions
15.	Real estate agencies
15.	Notaries
17.	Auction
18.	Auditors
19.	Exchange offices
20.	Securities dealers

PART 2 – ASSESSMENT OF THE VULNERABILITY OF LEGALIZATION OF PROCEEDS OF CRIME IN PARTICULAR SECTORS OF THE NATIONAL ECONOMY

2.1. BANKING SECTOR

GENERAL INFORMATION ON BANKING SECTOR IN THE SLOVAK REPUBLIC

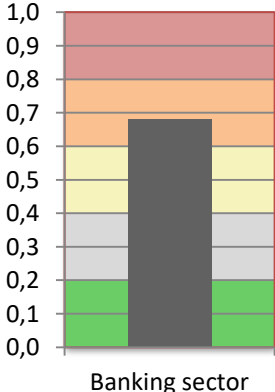
In Slovakia, the banking sector is relatively saturated and stable. During the period under review, 27 banks were operating on the Slovak financial market. Out of this number there were 10 banks, 13 branches of foreign banks, 3 building societies and 1 savings and credit cooperative.

Banks operating in SR offer a standard wide portfolio of products for their clients, whether they are natural persons or legal entities (irrespective of the size of the company). Most banks provide their products and services for both of the above client categories, only some of them specialize solely in natural persons or legal entities. In both cases, however, clients use modern technologies allowing remote communication with banks - "Internet banking", bank applications in mobile phones and smart banking devices, and a wide range of payment cards.

At the end of the period under review, the total assets of entities operating in the banking sector had a 90% share of GDP in the SR. The total value of the assets was EUR 69,011 million. EUR. The banking sector achieved a cumulative profit of EUR 626 million, representing an increase of 13.1% compared to the previous period (2014).

BANKING SECTOR VULNERABILITY

The overall vulnerability of the banking sector in the Slovak Republic was based on the evaluation of the collected information and data at a medium-high level, a numerical expression of the vulnerability level of 0.68 – please see the graph.



PROCEDURAL VULNERABILITY

In the context of the evaluation of the procedural aspect related to the performance of the activities and internal processes of individual entities in the banking sector as well as the supervisory and control authorities, it can be stated that the negative impact on the overall level of vulnerability and thus the most gaps were identified in the following areas:

- Effectiveness of supervisory/control procedures and methods,
- Knowledge of employees of the banking sector entities on AML measures,
- Existence and enforcement of administrative sanctions,
- Effectiveness of monitoring and reporting unusual transactions,
- Effectiveness of the procedures of the banking sector entities in compliance with the legislation,
- Existence and enforcement of criminal sanctions,
- Availability and access to beneficial ownership information, and
- Availability of independent information resources.

Effectiveness of supervisory/control procedures and methods

The FSJ is primarily authorized to exercise control of the statutory AML/CTF obligations under the conditions of the SR. In the case of entities (obliged entities) subject to supervision by the NBS, the law also allows the execution of the AML/CTF compliance check to be performed by the competent NBS supervisory authorities.

Control of the performance of obligations laid down by the AML/CTF Act is one of the strategic tasks and activities of these bodies. It is not only the control or supervision itself ("on-site" or "at a distance"), but also providing training, issuing guidelines and providing the interpretation of relevant provisions of the said Act.

A negative phenomenon adversely affecting not only on the control/supervision but also the above activities, is deeply understaffed FSJ and NBS in this area.³⁴ The ratio of the number of FSJ members and NBS employees to the number of entities in the banking sector is disproportionate. A negative impact was also found in the assessment of the planning and frequency of controls and supervision, the introduction of risk-oriented controls and supervision. In this respect, it is necessary to develop a set of measures (in the form of a methodology) assess and determine the risks of individual entities in the banking sector. Relevant information should be obtained through:

- a) Regular assessment of the level of AML/CTF systems³⁵ of banking sector entities based on the so-called self-assessment,
- b) Information and knowledge resulting from received UTR reports, and
- c) Information received in the performance of other tasks of the FSJ or the NBS.

³⁴ This fact, particularly from the point of view of the FSJ, can be considered as expressly horizontal (cross-sectional) since it directly affects all types of obliged entities.

³⁵ AML/CTF system of the obliged entity: a set of organizational, technical, methodological measures aimed at preventing and detecting the legalization and financing of terrorism.

However, the effective implementation and the implementation itself of risk-oriented controls and supervision also assumes the improvement of mutual cooperation between the FSJ and the NBS, which is based on the already existing Agreement on mutual cooperation between the National Bank of Slovakia and the Ministry of Interior of the Slovak Republic. The cooperation of the FSJ and the NBS would also make the joint control (supervision) more effective in a substantial way. There is currently no legal limitation on its implementation, but a higher initiative and overcoming organizational and personal contradictions are needed.

Knowledge of employees of the banking sector entities on AML measures

Employee training is a basic prerequisite for effective implementation and application of AML/CTF measures at individual levels within entities operating in the banking sector. In view of the dynamic development of individual areas of society, including anti-social activities, strong emphasis must be placed on regular and continuous training of employees.

For this reason, the risk assessment gave special attention to the area of provision and verification of acquired knowledge by the relevant staff. In addition to support and leadership (in the form of encouragement) in self-education, it is necessary to revise the current approach of the banking sector entities to education, but especially to the examination of knowledge. The training methods applied by the banking sector entities can be evaluated as standard, with respect to frequency and progress.³⁶ Employee training usually takes place in the bank's own direction. Only in isolated cases a banking sector entity asked the FSJ or NBS for cooperation. On the basis of the training provided, banks assessed the level of education of its employees at a medium-high level (7.76 points on a scale of 1 – weakest level of knowledge to 10 – excellent level of knowledge). In spite of the said positive features, however, it is necessary to change the approach to employee testing. A relatively inconsistent approach to employee testing was identified when comparing individual entities in the banking sector. In case of unsuccessful completion of the test, the employee is allowed to repeat the test from one repeated attempt to an unlimited number of attempts, where the model with an unlimited number of attempts prevailed. Such an approach can lead to benevolence in the training and continuous education of employees, and last but not least, this may have a negative impact on the reporting obligation. However, making the testing conditions more stringent and the setting of restrictive measures for repeated unsuccessful tests, appear to be appropriate countermeasures. Another shortcoming in education is the insufficient cooperation of the entities with the FSJ and NBS representatives, as well as the uneven dynamics of updating the education process in individual banks in terms of the organization and content.

³⁶I. The educational process is divided into three types of training:

- a) Initial training for new staff,
- b) Regular annual training for permanent staff,
- c) Additional thematic (ad hoc) training for selected groups of staff (management, AML/CTF specialists, lawyers, etc.)

II. The educational model is divided into two parts:

- a) theoretical (e-learning, class-room training),
- b) practical - verification of knowledge by testing

Existence and enforcement of administrative sanctions

The FSJ and the NBS have the statutory mandate to impose administrative sanctions for the violation of AML/CTF obligations. The scope of the sanctions available to those authorities cannot be considered sufficient. Financial penalties (sanctions) and remedial measures do not fully comply with international standards in this area. A shortcoming is mainly the impossibility of imposing a sanction, and hence attribution of direct liability for the detected violation on specific employees of the controlled entities, including the members of the governing bodies of the bank responsible for the AML/CTF area. This does not call into question the meaning of the so-called recourse proceedings, but such a measure would certainly contribute to the higher effectiveness and targeting of the sanction (as a means of remedy).

The approach of authorities to sanctions is also inconsistent. Although the FSJ imposes fines but their amount is sufficiently deterrent and does not prevent certain entities of the banking sector from repeatedly violating (also seriously) the statutory AML/CTF obligations. The NBS prefers remedies and less often imposes fines which are in lower bands, which in principle leads to a more benevolent approach of controlled entities in relation to the removal of identified deficiencies in the activity. In the period under review, the NBS imposed only two pecuniary penalties for a detected violation of the AML/CTF obligations, which may have an adverse impact on the level of vulnerability. In connection with the introduction of risk-oriented control or supervision it is advisable to review the amount and type of sanctions imposed.

Under the Banking Act, the NBS has the possibility of imposing a wider range of sanctions than the FSJ, including the possibility of imposing a fine on a member of the board of directors, a member of the supervisory board, a branch manager, an official receiver and a proctor. In case the bank is managed by a person other than the aforementioned one or a certain person has a key function in the bank, also in such cases, the NBS is entitled to impose a pecuniary penalty.

Effectiveness of monitoring and reporting unusual transactions

Monitoring and subsequent reporting of UTRs is the basis for the effective functioning of the AML/CTF system in the SR. The results are closely linked to the work and tasks of the FSJ. At the same time, it belongs to the strategic AML/CTF obligations of obliged entities. In the context of technical provision of client and transaction monitoring, a major part of entities under review uses automated monitoring systems and high-quality information systems, while a minor part of entities under review uses monitoring through semi-automated systems or manual provision. However, it should be noted that the diversity of established systems does not pose a significant risk of legalization. The entities under review have basically adapted (and continuously adapt) their information systems to the extent of the products and services provided in terms of their risk level.

However, a fundamental and persistent negative impact in this area is the insufficient application of due diligence - customer due diligence and enhanced due diligence. These deficiencies in principle concern all entities in the banking sector and have the so-called

cascading effect, which can lead to a reduction in the efficiency of FSJ activities. The deficiencies are manifested especially in the verification of the origin of clients' funds, in determining the purpose and nature of the transaction or business relationship. Banking sector entities inadequately assess the riskiness of their clients, resulting in an inappropriate relationship between "standard" and "increased" risk clients³⁷.

A particular defect in the evaluation of monitoring quality is the establishment of a business relationship with a client without his physical presence and the non-application of enhanced due diligence in the period under review. Based on the data provided by the entities under review, it can be prejudiced that, in particular, the so-called Internet banks (banks that do not have a network of stone branches) applied only customer due diligence. The manifestation of the so-called cascading effect of the said deficiencies is the reduced quality of recognition and reporting of unusualness in behavioural patterns and in operations performed by clients (one-time clients) of the entities under review.

It can be concluded from the information available under the NRA that a large number of entities operating in the banking sector prefer their own economic and commercial interests, which in many cases outweigh the obligation to comply with the AML/CTF legislation. This can also have an impact on the exchange of relevant information and the mutual cooperation of the banking sector.

Effectiveness of the procedures of the banking sector entities in compliance with the legislation

The statutory obligation of each obliged entity is to develop and update an internal regulation framework, the so-called AML/CTF programme³⁸. The application of the risk-oriented approach in this case is a prerequisite for its high-quality preparation. An important element in ensuring compliance with the law is the transparent division (and separation) of competences and responsibilities for the AML/CTF area at the top level and other levels of the banking sector³⁹. All entities under review have a unit⁴⁰ in place which is responsible for the AML/CTF area, which performs tasks resulting from the reporting duties and ensures communication with the FSJ or the NBS. Despite the fact that International Standards (FATF Recommendations) require the establishment of such a department at the management level, NRA findings indicate that not all entities meet this requirement. However, in this context, it should be noted that neither the legislation effective during the period under review required from obliged entities the establishment of an AML/CTF unit at the managerial level. Another defect, but this time fully in the powers of the management of the banking sector, is the staffing of the efficient execution of AML/CTF tasks. Part of the entities under review have insufficient staff who should be able to perform all obligations. The deficiency is also absent or low frequency of internal (and external) audits associated with AML/CTF processes in individual entities.

³⁷ This statement supports the practice and experience of the members of the team responsible for evaluating the banking sector and the results of the analysis of the audit findings and the material (content) aspect of UTR reports received.

³⁸ The AML/CTF Act defines this framework as a „programme of its own activity of an obliged entity“ and clearly specifies its content (please see more in § 20).

³⁹ AML/CTF area must be separated and independent of banking sector business units.

⁴⁰ The so-called „compliance officer“ or „appointed person“.

Existence and enforcement of criminal sanctions

The system of law of the Slovak Republic distinguishes the criminal liability of natural persons⁴¹ and the criminal liability of legal persons⁴². However, in the period under review, it was not possible to assess the availability and enforceability of legal regulations governing the criminal liability of legal persons since the law in question became effective only on 1 July 2016. The ability of the system to distinguish and effectively apply individual sanction regimes within the powers of FSJ, NBS and LEAs and courts is a challenge to future justice practice.

In relation to natural persons as (potential) perpetrators, it can be stated that criminal sanctions are available and sufficient, but in practice they are only applicable in very rare cases. Until now, sporadic cases have been reported when a criminal prosecution was initiated against a bank employee in the event of serious violations related to the performance (or non-performance) of AML/CTF obligations. Although raising the awareness of the banking sector towards employees is performed on a regular basis, the general awareness is not adequate to the seriousness and possible impact on their professional, and in the case of a final conviction decision, on their private life. This means that the current regime of criminal sanctions does not have the capacity to positively influence the behaviour of individuals.

Availability and access to beneficial ownership information

The availability of information on beneficial owners of legal entities (BOs) registered in the Slovak Republic is insufficient. At the time of the evaluation, this information was not kept in any central register. The entities of the banking sector must therefore rely on the manual acquisition and processing of information about the beneficial owners of their clients, on external databases offered by companies operating in the field. However, these external databases contain information obtained on a voluntary basis from the legal entities concerned.

However, in general, banking sector entities find the necessary information through "Know Your Client" questionnaires. This information is subsequently verified through identification documents from a legal entity or publicly available sources. In this context, appropriate legislative and technical measures should be taken at national level resulting in a database of beneficial owners of legal entities with a statutory obligation to provide timely and up-to-date information.

Availability of independent information resources

With respect to the shortcomings identified in verifying the beneficial owners of legal entities, it should be noted that despite the availability of independent information sources,

⁴¹ Act no. 300/2005 Criminal Act, as amended.

⁴² Act no. 91/2016 on Criminal Liability of Legal Persons, as amended.

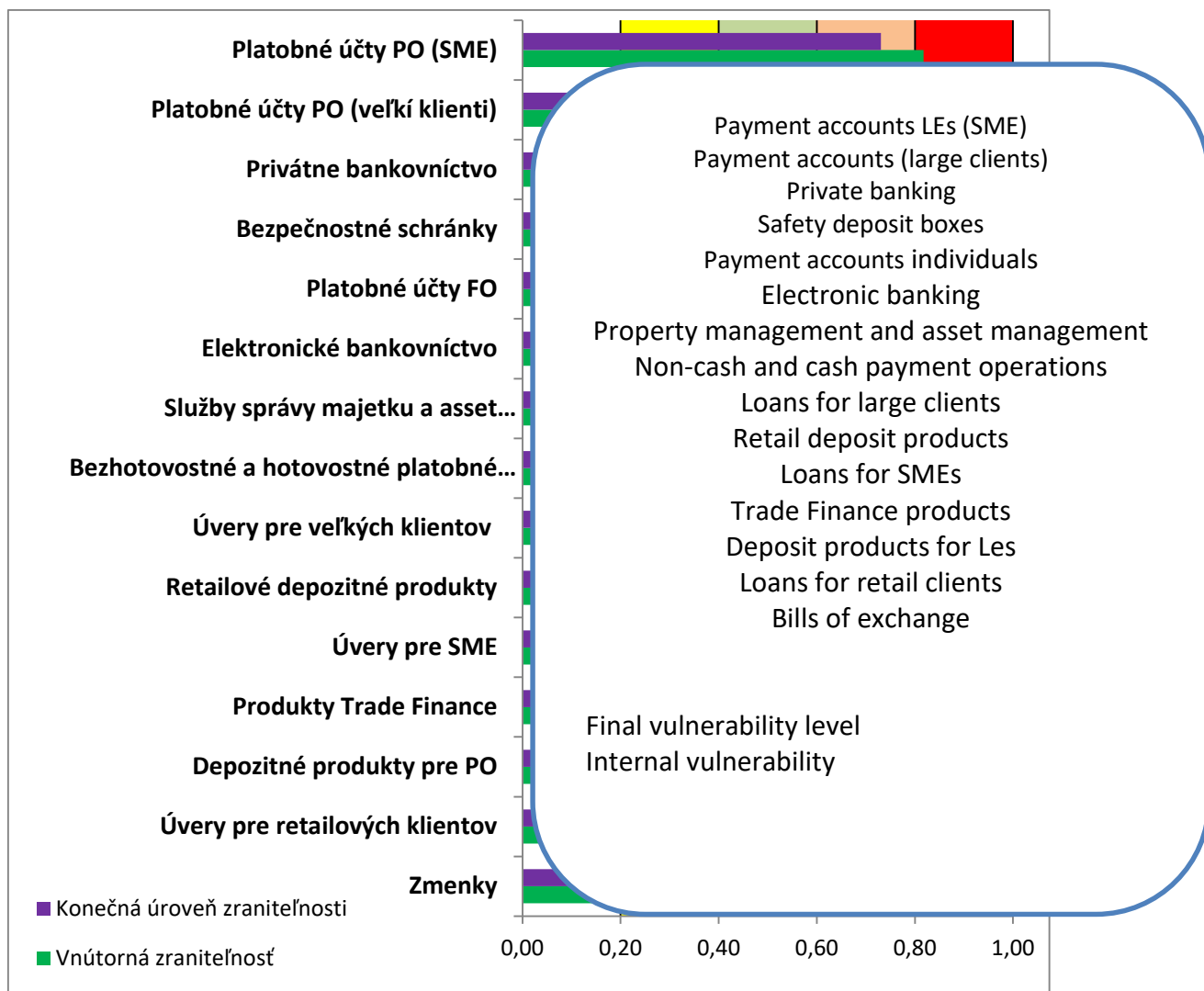
banking sector does not use the sources insufficiently to obtain additional information. We also note the absence of exchange of information between individual entities of the banking sector, in particular the exchange of negative information about banks 'risky clients and information on clients' fraudulent activities.

PRODUCT VULNERABILITY

For the purpose of objectively assessing the vulnerability of banking sector entities, it is necessary to provide a detailed assessment of the products and services provided. The results of such an assessment are key to identifying possible vulnerabilities of the products and services provided by the banking sector. These results are also an important element in the creation of risk-oriented supervision or control. At the same time, it is necessary for the banking sector entities to apply and take into account them in their own "self-assessment" mechanisms.

15 most frequently used products and services were evaluated within the Slovak banking market during the implementation of NRA. The activities of the working group mainly focused on the factors of internal vulnerability of the following products and services:

- Private banking
- Retail deposit product
- Deposit products for legal entities
- Credit products for retail clients
- Credit products for clients (small and medium-sized enterprises)
- Credit products for large corporate clients
- Payment accounts for individuals
- Payment accounts for legal entities (small and medium-sized enterprises)
- Payment accounts for legal entities (large corporate clients)
- Non-cash and cash payment operations
- Bills of exchange
- Property management and asset management services
- Trade Finance products
- Electronic banking
- Safety deposit boxes



The final vulnerability of the individual products provided

The results of an assessment of products within the NRA show a wide range of vulnerability levels for particular products and services – ranging from low to high. **A low level of vulnerability**, which means a low risk of the misuse of a specific product for legalization purposes was found for bills of exchange. On the other hand, **a high level of vulnerability**, which means a high risk of the misuse of a particular product for legalization purposes, has been detected in the payment accounts of legal entities (small and medium-sized enterprises). For NRA purposes, we provide below a detailed summary of products and services whose level of vulnerability has reached a level of medium – medium-high – high.

Payment accounts for legal entities (small and medium-sized enterprises)

Rating: high level of vulnerability

Payment accounts of legal entities (small and medium-sized enterprises) belong to the most significant and most widespread products provided by banks for this client group. It is the primary tool through which funds are entered into a legal banking system. From the

internal features of the product, as well as its direct relation to other products and services of the bank, it is necessary that banks consistently increase prudence in relation to clients and their deposits.

To determine the level of product vulnerability, the following attributes of the product were evaluated:

a) Cash transactions

From the point of view of allocation of the funds of the representatives of the private business, the primary focus is on the largest banks operating in the Slovak Republic. Other banks (including banks whose target group for products and services are legal entities) manage a lower order volume of funds intended for or coming from business activities.

Volume of all cash deposits/withdrawals on accounts of LEs at all banks in the SR in the EUR /ths. EUR/					
Clients - Legal entities:	2011	2012	2013	2014	2015
Cash deposits	14 518 633	17 262 930	16 848 394	16 555 517	16 394 832
Cash withdrawals	9 542 928	11 479 487	11 284 866	10 342 749	10 200 236

As shown in the above table, at the end of the period under review, there was a slight drop in the amount of cash deposits or withdrawals. The total volume of deposited funds reached roughly 16 bil. EUR⁴³. Compared to transactions executed through payment accounts of natural persons, a larger share of deposits was recorded, in comparison with withdrawals, in order of 1.5 times the volume.

Based on the information available and the overall tax and payment management, it may be assumed that part of the funds allocated to payment accounts of legal entities may be related to tax offenses (in particular tax evasion, tax non-payment, tax fraud, etc.).

An average transaction amount is in the order of 1,000 to 10,000 EUR. Compared to transactions executed on payment accounts of individuals, it is significantly higher, but it does not represent an increased risk from the point of view of legalization.

Following the above stated information, the funds placed within the said product represent a high risk.

b) Client profile

In general, banks assess small and medium-sized enterprises as low (standard) risk clients, but this does not correspond to the results of the analysis of the content of UTR reporting and the nature of the financial crime development. According to the information available, the most frequently executed transactions that are part of carousel fraud or fraud carried out in connection with excessive VAT deductions are precisely through the business accounts of small and medium-sized enterprises. In addition, there are often cross-border transfers to risky countries or, countries known as tax havens (offshore countries). A specific category in terms of "business" of the client are business entities dealing with the special-purpose

⁴³ The said amount of funds accounts for roughly 21% of GDP in the SR.

establishment and cancellation of business companies, including shell companies as well as entities using the virtual office of such companies. On the basis of the facts ascertained, the profile of the client is a high risk characteristic of the product.

c) International transactions

With respect to the frequency and volume of funds transferred, international transactions represent a medium risk. Factors affecting the identified level of risk are in particular transfers to tax havens (offshore countries), risky countries as well as transfers within the EU, in many cases serving to hide the illegal origin of funds and make it more difficult for the competent authorities to verify them.

Payment accounts for legal entities (large corporate clients)

Rating: medium-high level of vulnerability

Payment accounts for corporate clients (large corporate clients) complement the portfolio of the most important and most widespread products provided by banks in relation to trade companies. Even in the case of large corporate clients, it is necessary that banks increase their prudence in relation to these clients and their deposits, given the characteristic features and characteristics of the product.

To determine the level of product vulnerability, the following attributes of the product were evaluated:

a) Product size and cash transactions

The allocation of the funds of large corporate clients is unevenly distributed in the Slovak banking market. The focus of business entities on the largest banks operating in the Slovak Republic was maintained for large corporate clients as for small and medium-sized enterprises, but the major difference is that smaller banks predominate compared to medium-sized ones. In other groups of banks, funds are placed in volumes of a lower order. In view of the above, as well as the investment potential of these clients, the volume of the funds invested poses a high risk in terms of potential legalization of proceeds of crime.

In relation to the use of cash operations, the risk is lower compared to small and medium-sized enterprises. In the case of large corporate clients, cash activities are used to a lesser extent and represent a medium risk. This fact can be justified by the characteristic features of the business activities of these entities.

b) Client profile

Client's general profile - a large corporation has a distinctly different character from a typical ownership structure of small and medium-sized enterprises. The ownership structure is made up of a large number of owners, whereas key owners with a large shareholding are large business companies. The minority is made up of owners – small and medium-sized enterprises and individuals. Characteristic features of corporations are: a defined

organizational structure, a transparent management scheme⁴⁴, internal policies and codes. To a minimal extent the ownership structure includes links to trade companies registered in business registers (or similar registers) in countries called tax heavens (offshore countries). The client's profile for the said product represents a medium risk of legalization.

With regard to the implementation of mandatory customer due diligence by banks, minor deficiencies have been identified than in the case of payment accounts for small and medium-sized enterprises. Insufficient implementation of mandatory due diligence is multiplied, in particular, in the identification of BOs for corporations with a large and complicated ownership structure and a high number of owners.

c) International transactions

-border transfers of funds are a frequent accompanying phenomenon of the business of large corporations. Business activities are in many cases focused on transnational markets, they establish branches in the region or in foreign countries. For these reasons, international transactions pose a medium-high risk.

General information on cash and non-cash transactions executed through payment accounts of legal entities irrespective of the product size parameter:

Cash transactions

Volume of all cash deposits/withdrawals on accounts of LEs at all banks in the SR in the EUR /ths. EUR/					
Clients - Legal entities:	2011	2012	2013	2014	2015
Cash deposits	14 518 633	17 262 930	16 848 394	16 555 517	16 394 832
Cash withdrawals	9 542 928	11 479 487	11 284 866	10 342 749	10 200 236

In relation to cash activities, the long-term prevalence of cash deposits compared to cash withdrawals was recorded. With respect to the identified threats of legalization in the Slovak Republic, it is possible to call the part of the funds thus deposited as proceeds (income) from criminal offenses of economic nature (especially tax and related criminal activity) that the potential perpetrators want to place and integrate through the legal banking sector.

Non-cash transactions

Volume of all non-cash credit/debit and cross-border transactions on accounts of LEs at all banks in the SR in the EUR /ths. EUR/						
Clients - Legal entities:		2011	2012	2013	2014	2015
Domestic transactions and SEPA payments	credit	345 484 024	471 440 186	567 174 032	608 410 922	575 558 720
	debit	368 724 403	486 740 182	587 131 707	622 181 878	604 554 890

⁴⁴ The management scheme usually consists of a board of directors, a supervisory board, an audit department, a compliance department, etc.

Cross-border in the EU	Payments to the SR	35 684 601	31 838 192	53 584 072	39 587 217	27 766 614
	Payments from the SR	45 355 580	41 317 932	60 991 077	47 748 523	45 281 636
Off-Shore countries	Payments to the SR	212 295	199 656	136 527	172 095	349 885
	Payments from the SR	479 874	429 421	383 115	375 264	546 578
High-risk countries	Payments to the SR	31 236	33 112	62 438	49 525	54 901
	Payments from the SR	95 989	67 247	207 027	176 218	286 064

a) Domestic payments:

- With respect to domestic payments, a generally increasing trend in the execution of debit domestic transactions was recorded.

b) Cross-border payments:

- In connection with the execution of cross-border payments, a higher prevalence of payments from the SR was recorded compared to payments to the Slovak Republic. The highest volume of funds was transferred to the Czech Republic and Hungary.
- The highest volume of funds transferred to the so-called tax heavens (off-shore countries) was recorded with respect to Cyprus, Switzerland and Liechtenstein.
- The highest volume of funds transferred to risky countries was recorded in relation to Bosnia and Herzegovina.

Technical properties of the product

When assessing the technical properties of the product "payment account for legal entities", the following risks were identified:

- Unlimited number of cash and non-cash transactions,
- Possibility of transferring funds abroad, including high-risk countries,
- Possibility to dispose of a payment account through remote access tools, and
- Possibility to establish a POS terminal for accepting card payments.

The level of vulnerability of the product is also adversely influenced by the insufficient application of mandatory customer due diligence (and, in some cases, enhanced due diligence) in relation to clients by banks. In cases where the commercial interests of banks outweigh the interest of the competent state authorities in developing a secure financial system, the level of vulnerability of the particular products provided proportionally increases.

Private banking

Rating: medium-high level of vulnerability

In Slovakia, Private Banking services are provided by eight banks. In terms of the allocation of funds, a greater part of funds is concentrated in three banks.

On the basis of the evaluation of information and data obtained from the NRA process, it can be concluded that banks applied a limited risk-based approach to assessing the risk profile of clients to whom private banking services were provided, to a very limited extent. Most banks consider such clients as regular retail clients, although private banking services are generally considered as posing an increased risk⁴⁵. The average transaction amount is in the order of ten thousand EUR. It is based, in particular, on the fact that the services are generally provided to clients with a certain influence, with a social influence with a possible relationship to politically active decision-makers, both centrally and regionally. At the same time, such a client has more possibilities of investing free funds in different products, in particular in terms of their volume, broader overview of investment options, higher acceptance of investment risk and, last but not least, above-standard advisory services.

In terms of cash use, a decreasing trend in the volume of cash deposits/withdrawals on personal and term accounts of private banking clients was recorded.

Volume of all cash deposits/withdrawals on personal and term accounts in all banks in the SR in the EUR /ths. EUR/						
Private banking clients		2011	2012	2013	2014	2015
Account type:	Transaction type:					
Personal (current)	Cash deposits	192 875	187 570	154 461	140 841	139 497
	Cash withdrawals	242 108	219 884	192 399	197 878	191 904
Term (saving)	Cash deposits	39 923	17 501	9 706	9 543	6 940
	Cash withdrawals	29 615	10 267	5 758	4 275	5 098

The negative consequence of the limited use of the risk-oriented approach is the absence of the duty to report on the part of banks. In this regard, it can be stated that banks apply insufficiently customer and enhanced due diligence measures, while at the same time there are shortcomings in the assessment, detection and reporting of unusual transactions. In order to remove the persistent deficiencies, it is necessary to review the bank's approach to private banking clients and to take specific measures aimed at reducing the vulnerability in the provision of the service.

The level of vulnerability of the product is also adversely influenced by the insufficient application of mandatory customer due diligence (and, in some cases, enhanced due diligence) in relation to clients by banks. In cases where the commercial interests of banks outweigh the interest of the competent state authorities in developing a secure financial

⁴⁵ Interpretive Note to the FATF Recommendation 10 „Customer due diligence" clearly states that private banking is one of the circumstances when assessing products, services, transactions (deals) or delivery channels used, with respect to which ML and TF risks are higher and therefore enhanced due diligence is necessary.

system, the level of vulnerability of the particular products provided proportionally increases.

Safety deposit boxes

Rating: medium-high level of vulnerability

The safety deposit box service provides only a limited number of banks operating in the Slovak Republic. As a rule, this service is provided only by larger branches, which have the appropriate technical, organizational and logistic conditions for this purpose. Despite the fact that the service is provided as part of banking activity, banks do not apply customer due diligence as defined in the AML/CTF Act. As a rule, only the client's identification (and verification of the identification) and the completion of the specimen signature is executed. The provision of the service in question is conditional on the conclusion of a contract for the lease of a safety deposit box between the client and the bank. The terms and conditions clearly state which items cannot be stored in the safety box. However, the contents of the safety deposit box are not subject to bank control.

On the basis of the information obtained, the following ML risks associated with the use of the safety deposit box service were identified:

- Banks have only a limited scope of information on the lessees of safety boxes, defects of proper performance CDD are apparent mainly in the absence of information on the purpose and nature of the business relation and the absence of continuous client monitoring,
- Safety deposit box service is provided without the obligation to have a bank account or a different account with the bank, or a different product or service, i.e. the bank does not have any information about the client (received based on CDD / KYC),
- Banks are not responsible for the contents of the safe box, do not check items and things stored in the safety deposit box,
- Bank does not perform CDD / KYC against third parties authorized by the lessee to handle the box, except for their identification (and verification of identification),
- The record of the lessees of safety boxes is generally kept in manual form and not in the banking information system,
- Absence of information on breaches of the conditions of use of the safety deposit box, in particular in the context of the legalization of proceeds of crime.

Although the application of the principle of discretion in the provision of a Safety deposit box is a basic prerequisite and a feature declared by the bank, paradoxically, this principle greatly increases the vulnerability of this service.

Payment accounts of individuals

Rating: medium level of vulnerability

Payment accounts of individuals belong to the most significant and most widespread products provided by banks for this client group. It is the primary tool through which funds are entered into a legal banking system. From the internal features of the product, as well as its direct relation to other products and services of the bank, it is necessary that banks consistently increase prudence in relation to clients and their deposits.

Volume of all cash deposits/withdrawals on accounts of individuals at all banks in the SR in the EUR /ths. EUR/						
Clients – Individuals:		2011	2012	2013	2014	2015
Personal (current)	Cash deposits	5 600 555	5 999 090	6 156 305	6 303 977	6 163 705
	Cash withdrawals	12 798 391	13 896 634	14 258 038	14 772 058	14 902 912

Despite the efforts of national and supranational bodies (such as the FATF, the MONEYVAL Committee) to reduce the level and the negative impact of the risk of the misuse of cash, the opposite trend was paradoxically reported for the Slovak banking market. Following the information in the above stated table, it can be stated that the volume of cash deposits on payment accounts has an increasing trend. A negative accompanying phenomenon, along with an increase in the volume of cash deposits, is an increase in the volume of cash withdrawals. At the end of the period under review, withdrawals accounted for in 2 to 3 times the volume compared to deposits. The total volume of cash withdrawals reached a level of roughly EUR 15 billion.⁴⁶ Cash transactions executed in connection with payment accounts represent a high risk of legalization.

Volume of all non-cash credit (domestic and SEPA) transactions on individuals accounts in all banks in the SR in the EUR /ths. EUR/						
Clients – Individuals:		2011	2012	2013	2014	2015
Credit		37 475 272	41 562 568	44 180 696	44 967 096	53 997 388

In connection with an increase in cash withdrawals, there was also a significant increase in non-cash transfers between payment accounts of individuals. These were executed in a total amount of roughly EUR 54 billion. A sharp increase in the volume of funds transferred could also be due to the introduction of the so-called SEPA payments⁴⁷, mainly in relation to cross-border transactions and, of course, real economic growth.

Volume of all non-cash credit/debit and cross-border transactions on individuals accounts in all banks in the SR in the EUR /ths. EUR/						
Clients – Individuals:		2011	2012	2013	2014	2015
Domestic transactions and SEPA payments	Credit	37 475 272	41 562 568	44 180 696	44 967 096	53 997 388
	debit	26 555 661	30 282 700	32 744 915	31 520 140	39 633 138

⁴⁶ The said amount of funds accounts for roughly 19% of GDP in the SR.

⁴⁷ SEPA – Single Euro Payments Area. Its aim is to unify the rules and standards in the execution of cross-border payments of funds in the EUR.

Cross-border in the EU	Payments to SR	353 524	705 273	868 464	981 576	1 170 049
	Payments from SR	613 857	722 565	1 102 604	1 147 812	2 084 432
Off-Shore countries	Payments to SR	31 686	28 101	25 895	20 186	32 518
	Payments from SR	17 072	24 235	19 233	19 987	21 246
High-risk countries	Payments to SR	927	2 744	2 735	1 295	1 883
	Payments from SR	1 404	1 425	2 057	2 562	2 905

On the basis of the data and data obtained, the following trends were recorded:

- a) Domestic payments: significant increase in credit payments,
- b) Cross-border intra-EU payments: at the end of the period under review, a significant increase in the volume of funds transferred from the Slovak Republic to EU countries, including a long-term steady trend with prevailing payments from the Slovak Republic. The highest amount of funds was transferred to the Czech Republic, Hungary and the United Kingdom of Great Britain and Northern Ireland.
- c) Cross-border payments with tax heavens (offshore countries): at the end of the period under review, a significant increase in the volume of funds transferred to the Slovak Republic, including the long-term steady trend with incoming payments exceeding outgoing payments. The largest amount of funds was transferred to Switzerland, Cyprus and Liechtenstein.
- d) Cross-border payment system with high-risk countries: a long-term increase in the volume of funds transferred from the Slovak Republic to Bosnia and Herzegovina.

The higher level of risk of payment accounts is due in particular to the following technical characteristics:

- Unlimited number of cash and non-cash transactions, including an unlimited limit,
- The possibility of cross-border transfers of funds (with the possibility of transferring funds to risky countries from the point of view of legalization or terrorist financing),
- The possibility to dispose of funds on a payment account through remote access tools (electronic banking, internet banking, mobile payments, payment cards), including the risk of delivery of remote access tools to the payment account to another (third) party,
- Wide range of client base profile,
- Insufficient implementation by the bank of customer due diligence measures (and inconsistent compliance of duty to report to the FSJ).

Electronic banking

Rating: medium level of vulnerability

Electronic banking is provided by banks simultaneously with payment accounts, irrespective of the fact whether they are payment accounts for individuals or legal entities. In principle, this is not a stand-alone service but only providing higher comfort to clients by the bank in managing funds on a payment account.

To determine the level of product vulnerability, the following attributes of the product were evaluated:

a) Product size

With regard to the characteristics of the electronic banking service, the assumption of a high concentration of payments was confirmed, especially in the largest banks operating in the Slovak Republic. The size of the product in relation to the legalization risk was difficult to assess due to its internal link to the bank account of the client of the bank which is subject to due diligence related to transaction monitoring. Given the volume of funds transferred by the electronic banking service and the overall shortcomings of banks in the implementation of CDD measures, it is possible to determine the level of risk at the medium level.

b) Client profile

By generalizing the results of the assessment client product profile, the payment account of individuals and the profile of the clients of the product, the payment account of legal entities – as these profiles are identical in the case of electronic banking, it is possible to determine the level of risk also at the medium level.

c) Average amount of transactions and the frequency of international transactions

Despite the fact that the assessment criterion and benchmark was difficult to determine in relation to the average amount of the transaction because they are products with a wider range, the risk level was assessed at a medium level. The Electronic Banking service enables clients to execute domestic transactions as well as transactions abroad in an unlimited volume. Some banks operating in the Slovak Republic have certain restrictions and limits, when the assistance of the headquarters is required if the limits are exceeded. In this case, the client is authorized to make transfers of funds up to the balance amount on the payment account. These facts concerning the frequency of international transactions represent a medium level of risk.

The peculiarity of the electronic banking service in terms of assessing its vulnerability is in the use of electronic banking. Since the essence of this service is the possibility of using the so-called remote access to a payment account, i.e. outside of the bank's premises (bank branches), protection against unauthorized handling of computer data cannot be ensured at the highest level, although developments in cybersecurity still go forward. The highest risk is associated with the use of technical devices, such as computers or mobile phones (smart-technical devices), where it is practically impossible to prevent the misuse of personal codes or passwords in the data transfer process or in the case of theft of these technical devices. At the same time, a significantly negative impact on the electronic banking service has the deliberate delivery of personal codes and passwords to an unauthorized person. These elements of vulnerability are closely related to fraudulent activities of the above character and they have a slightly increasing trend based on an analysis of the information obtained

during the performance of the FSJ tasks. From a typological point of view, fraudulent activities include „phishing⁴⁸“, „pharming⁴⁹“, „vishing⁵⁰“, „spoofing⁵¹“ etc.

Property management and asset management

Rating: medium level of vulnerability

The service is provided by 7 banks out of a total of 27 banks operating in the Slovak Republic. Also, in this case, the largest banks operating in the territory of the Slovak Republic manage the highest amount of funds through the service. Other banks manage volumes of a lower order.

The Property Management and Asset Management service is provided for both individuals and legal entities. In terms of client profiling in relation to natural persons, private banking clients dominate these services to whom the services are provided by banks on the basis of a mandate contract. Private banking clients, even in the case of asset management, represent a high level of legalization risk. In relation to the provision of the service in question to legal entities, the risk is low, as they are supplementary pension companies, pension management companies, securities dealers, etc. Generally, clients pose a medium risk of legalization.

Cash activities with respect to the internal characteristics of asset management services pose a low risk. Funds are deposited via a payment account, so cash transactions are at a minimum level. The measures to verify the origin of the funds should therefore be taken before the funds are deposited into the payment account itself. For these reasons, the average transaction amount poses a medium-low risk.

The asset management service provides a significant opportunity to invest in assets both in this country and abroad. In this context, international transactions represent a medium-low risk, but the investment possibility represents a medium risk of legalization.

DETERMINING PRIORITIES IN THE ACTIVITIES OF THE CONTROL AND SUPERVISORY AUTHORITIES

⁴⁸ Phishing: the fraudulent attempt to obtain sensitive information from the user through fake emails or websites (the computer or mobile of a user is deliberately attacked by a virus or fraudulent application for the purpose of subsequent unauthorized transfer of funds from the account without the consent and knowledge of the account holder).

⁴⁹ Pharming: the fraudulent attempt to obtain sensitive information from the user through controlled websites (redirecting the name of www site to another address through which data may be misused and then funds may be withdrawn from the account of the injured).

⁵⁰ Vishing: form of fraud where perpetrators attempt to obtain sensitive information from the client using a phone call (individuals are tricked into revealing passwords for Internet banking, payment card numbers or other personal data).

⁵¹ Spoofing: fraud associated with the use of false identity (identity manipulation through two-party communication for the purpose of tricking the user into giving up and subsequent misuse of confidential information from the user).

The shortcomings identified during the implementation of the NRA have a greater or lesser impact on the functioning of the banking sector. In order for the control and supervisory bodies to be able to perform their tasks and responsibilities effectively, it is necessary to determine the level of priority for each of these areas. Identifying priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these bodies with a direct impact on the activity of the banking sector entities. The priority was determined by assessing the impact of identified shortcomings on the banking sector as a whole, in particular, its importance, nature and types of activities (operations) executed within this sector.

Priority level	Area
1.	Effectiveness of supervisory practices and methods
2.	Knowledge of bank employees about AML measures
3.	Existence and enforcement of administrative sanctions
4.	Effectiveness of UTR monitoring and reporting
5.	Effectiveness of the bank responsible for compliance
6.	Existence and enforcement of criminal sanctions
7.	Availability and access to beneficial ownership information
8.	Availability of independent information sources

PROVISION OF FINANCIAL INCLUSION PRODUCTS

By expanding the availability of bank products, especially payment accounts, for the benefit of the largest group of consumers, the state fulfils its tasks not only in the area of social policy but, above all, in the protection of low-income and otherwise underprivileged groups of the population from their possible misuse for legalization purposes. The statutory obligation for free provision of selected types of banking services was introduced in Slovakia in 2013.

Banks and branches of foreign banks are obliged to provide individuals with a regular residence in the EU with the so-called basic banking product free of charge, but subject to the following basic conditions:

- Age above 18,
- Net monthly income not exceeding 400,- EUR,
- Total annual turnover not exceeding 5,600,- EUR, and
- The client does not have a payment account in another bank or branch of a foreign bank.

In the period under review, only 13 banks and branches of foreign banks provided their clients with the establishment and administration of the so-called basic banking product. At the end of the period under review, **216 individuals** were using this option. An overview of open and closed payment accounts is provided in the table below.

Year	2013		2014		2015	
Status	Open	Closed	Open	Closed	Open	Closed
Number of basic banking products	104	26	163	57	77	45

Since the applicable legislation de facto limits the content of products and services provided within the basic banking product, bank clients and branches of foreign banks preferred standard payment accounts that are more favourable to them. In this case, the client could also use the payment account free of charge, but with a larger range of services provided in a package of services.

In the case where a bank or a branch of a foreign bank provides its client with a basic banking product, the mandatory customer due diligence is performed to the same extent and on the basis of the KYC principles as for other products. Neither AML/CTF Act nor any other special regulations specify any exception in this case. Banks and branches of foreign banks have adequate monitoring mechanisms in place to detect unusual transactions.

In the period under review, the FSJ did not investigate any suspicion of crimes committed in connection with the use of the basic banking product. Likewise, none of the banks or

branches of foreign banks reported to the FSJ an unusual transaction executed through the relevant product.

With regard to the total amount of opened basic banking products, their internal characteristics and the measures taken by banks and branches of foreign banks, it can be stated that the vulnerability of financial inclusion products in the Slovak conditions is **low**.

2.2. SECTOR OF NON-FINANCIAL BUSINESSES AND PROFESSIONS

GENERAL INFORMATION ON SECTOR OF NON-FINANCIAL BUSINESSES AND PROFESSIONS

The sector of non-financial businesses and professions was the most numerous in terms of the number of rated categories. A total of 14 categories with a very different occupational focus were evaluated. The reason for such a wide range of NRA was the fact that this was the first assessment in the SR, the results and findings of which will be used by relevant bodies in the application of the risk-oriented approach in the control, methodical activity, as well as in the updates of the NRA itself.

The following 14 categories of DNFBPs were assessed according to the statutory definition of the obliged entity resulting from the AML/CTF Act:

- i) Lawyer,
- ii) Notary,
- iii) Court distrainer,
- iv) Administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings,
- v) Auditor,
- vi) Tax advisor,
- vii) Accountant,
- viii) Organizational and economic advisor,
- ix) Service provider of property management or a company service provider,
- x) Postal undertaking,
- xi) Gambling operator,
- xii) Legal entity or a natural person authorized to mediate sale, rent or purchase of real estate,
- xiii) Legal entity or a natural person authorized to trade in precious metals or gemstones, and
- xiv) Legal entity or a natural person authorized to operate a pawnshop.

A negative phenomenon in the non-financial sector is the fact that the competent authorities do not have the exact number of obliged entities in this area. Businesses have in many cases several licenses (unqualified (notifiable) trade) based on which they can be considered an obliged entity, but some do not use some of licenses at all.

This long-lasting negative phenomenon is visible especially in the following categories of the non-financial sector:

- Organizational and economic advisor,
- Accountant, and
- Legal entity or a natural person authorized to mediate sale, rent or purchase of real estate.

The table below shows the total number of existing licenses issued in the non-financial sector during the period under review.

Year/category	2010	2011	2012	2013	2014	2015
Service provider of property management or a company service provider	-	-	-	-	-	-
Accountant	70 774	72 563	74 984	79 674	122 394	128 328
Postal undertaking	20	20	22	23	23	21
Organizational and economic advisor	106 392	167 275	-	-	293 065	307 081
Gambling operator	318	318	319	320	324	316
Dealer in Precious Metals and Stones	325	322	31	301	293	275
Pawnshops	-	-	-	-	4 026	7 198
Notary	337	340	340	340	344	342
Lawyer	4 666	5 044	5 398	5 104	6 292	5 700
Tax advisor	897	904	905	899	951	933
Administrator	-	-	-	484	503	521
Auditor	824	820	807	830	835	773
Real estate agency	35 099	35 427	35 585	34 472	57 256	58 555
Court distrainer	-	-	-	309	345	337

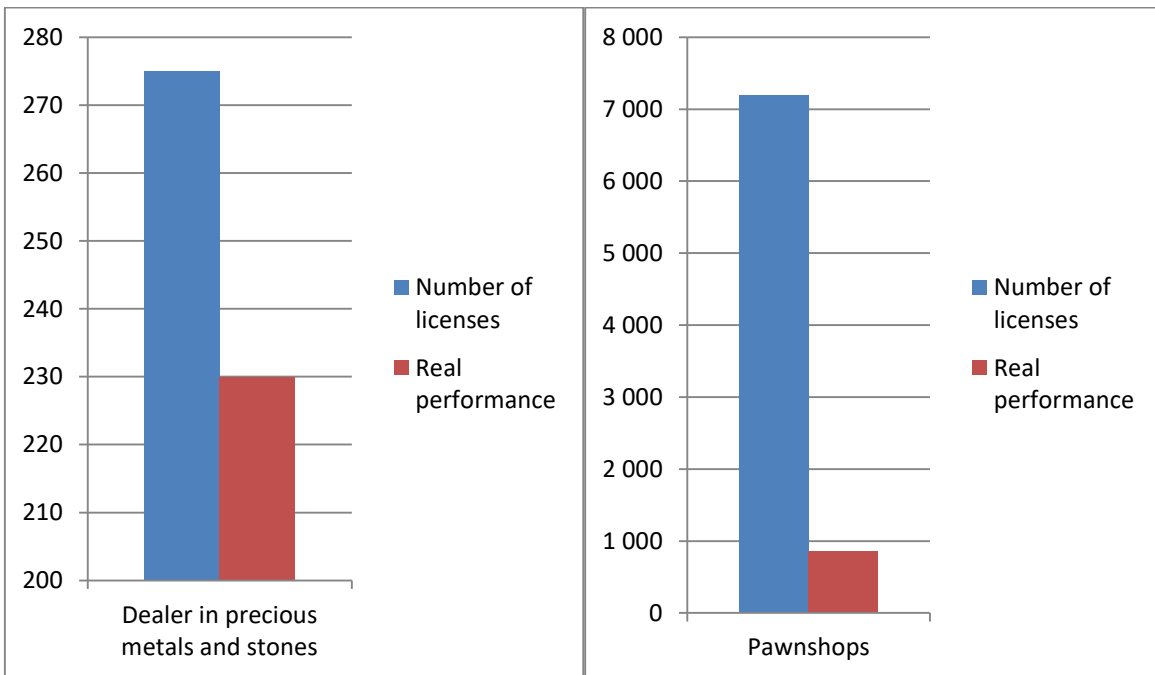
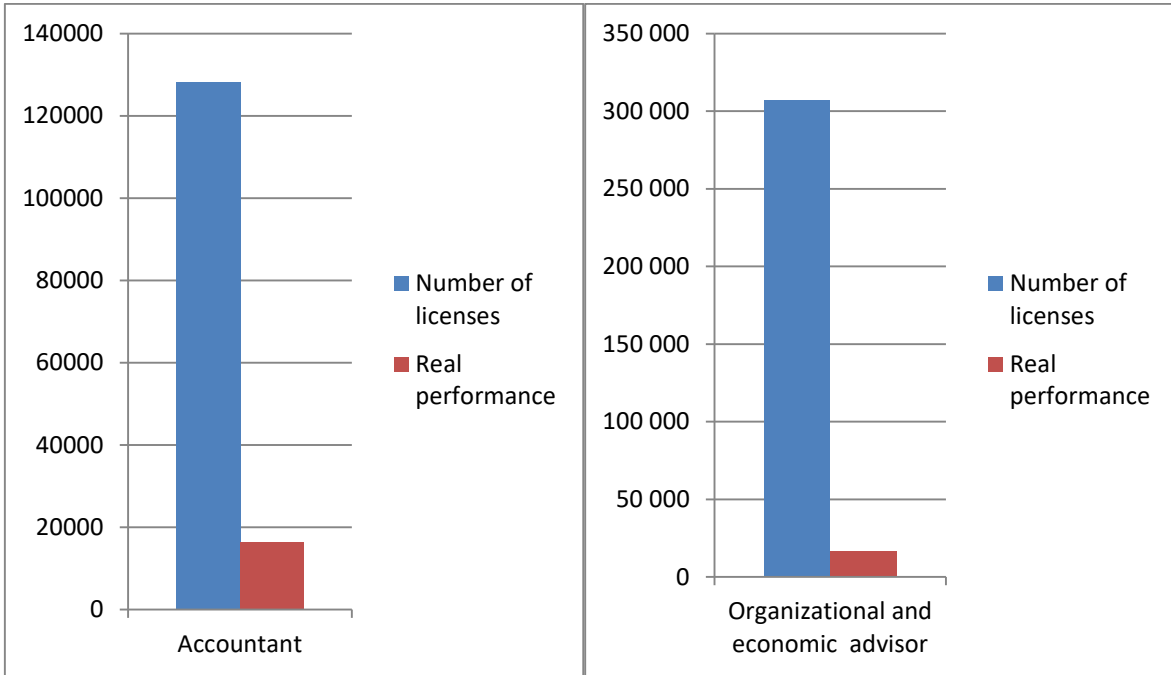
However, according to the information received from the FD SR on the submitted tax returns (main subject of activity), the structure of the non-financial sector is different in terms of the number.

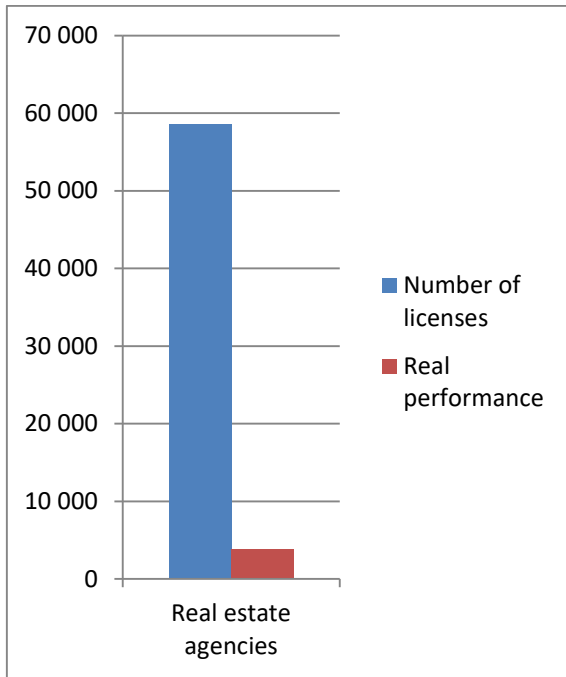
In this respect, the following categories of the non-financial sector are most wide-spread.

- Accountant,

- Pawnshop
- Organizational and economic advisor,
- Lawyer, and
- Legal entity or a natural person authorized to mediate sale, rent or purchase of real estate.

Year	Accountant		Organizational and economic advisor		Dealer in Precious Metals and Stones		Pawnshops		Real estate agency	
	Trades Licensing Offices SR	FD SR	Trades Licensing Offices SR	FD SR	Trades Licensing Offices SR	FD SR	Trades Licensing Offices SR	FD SR	Trades Licensing Offices SR	FD SR
2011	72 563	15 414	167275	10 716	322	248	-	806	35 427	3 221
2012	74 984	15 893	-	11 931	31	264	-	792	35 585	3 424
2013	79 674	16 377	-	13 268	301	246	-	801	34 472	3 689
2014	122394	17 216	293065	14 859	293	24	4026	947	57 256	3 880
2015	128328	16 484	307081	14 698	275	230	7198	857	58 555	3 832

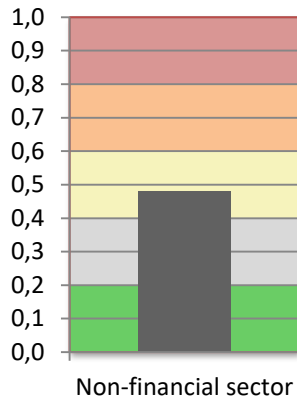




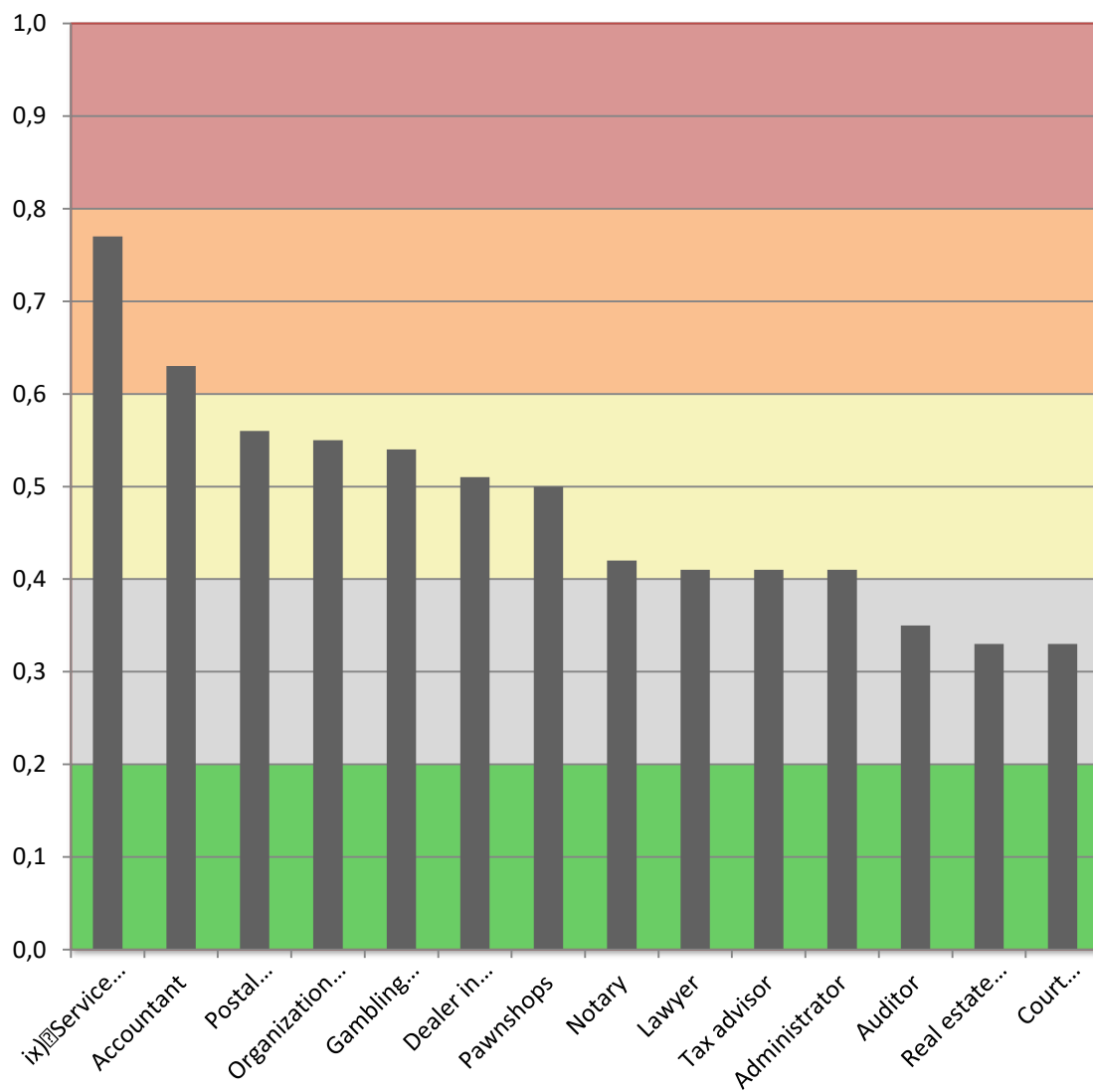
In general, the high total number of non-financial sector businesses, and the unknown number of actually active obliged entities, causes a high level of vulnerability in terms of communication, issue of guidelines and notices in relation to the FSJ and the MF SR. It is also a vulnerable place in terms of both AML/CTF control and general supervision.

VULNERABILITY OF THE SECTOR OF NON-FINANCIAL BUSINESSES AND PROFESSIONS

The overall vulnerability of the non-financial sector in the Slovak Republic was based on the evaluation of the collected information and data at the **medium level**, a numerical expression of the overall level of vulnerability at 0.48 – please see the graph.



Comparative graph of the vulnerability levels of individual non-financial businesses professions



PROCEDURAL VULNERABILITY

VULNERABILITIES IN THE SECTOR OF NON-FINANCIAL BUSINESSES AND PROFESSIONS

The following vulnerabilities were identified by assessing the procedural aspect related to the performance of the activities and internal processes of the non-financial sector businesses as well as the supervisory and control bodies:

- Insufficient knowledge of the AML/CTF area and staff training,
- Shortcomings in customer due diligence and in identification of the origin of the client's funds,
- Lack of supervision,
- Demonstrating the integrity of the staff,
- Inefficient recognition and monitoring of UTRs,
- Inefficient entry control mechanisms when issuing a license, or when registering,
- Availability and enforcement of criminal and administrative sanctions,
- Possibility of setting up an unlimited number of companies,
- Conduct of activities without transparent trade license,
- Non-performance of internal controls,
- Failure to keep written documents,
- Non-use of the possibility of information exchange under AML/CTF Act,
- Use of cash payment operations,
- Insufficient compliance functions,
- Absence of independent information sources,
- Deficiencies in the understanding of the risks of the profession, and
- Absence of the BO register.

Detailed analysis of selected vulnerabilities in the non-financial businesses and professions sector

a) Effectiveness of supervisory/control procedures and methods

- A serious vulnerability is the low number of FSJ members responsible for AML/CTF control over the long term, poor technical equipment, budget and experience gained mainly by self-education. With respect to the activity of the relevant FSJ department, the level of vulnerability is adversely affected by the failure to enforce a clear policy, due to fluctuation of the managerial staff and the absence of plans to establish and introduce robust changes in the rules currently in force with respect to obliged entities. There is also no exchange of information on ML/TF options and on new forms of phenomena in individual sectors among financial intelligence units.

- In this context, it is also necessary to stress that the execution of AML/CTF controls, with the exception of gambling operators, is entirely within the competence of the FSJ. As in the case of the sector of Other financial institutions, there is also a clear disparity between the number of FSJ officers responsible for the of control and the number of obliged entities.

- Another vulnerability in the performance of the AML/CTF control is the fact that the FSJ did not carry out any control in the following non-financial sector businesses, over the period under review:

- Postal undertaking,
- Administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings.

One control during the period under review was performed with the Tax Advisor and the Auditor.

- The Ministry of Finance has statutory powers with respect to the AML/CTF Act to perform AML/CTF supervision in relation to gambling operators.

- Another vulnerability influencing the control by the FSJ and the supervision by the Ministry of Finance is the absence of mutual cooperation, exchange of information (mutual training) and exercise of joint controls (supervision). No joint control was recorded with the gaming operator during the period under review.

b) Insufficient knowledge and awareness of the ML/TF risks and their management

- The information available shows that, even in the case of the non-financial sector, a significant vulnerability is insufficient education of staff and their training. Insufficient knowledge is particularly evident in the lack of implementation of mandatory customer due diligence measures, which implies that the obliged entity does not know its clients and does not obtain information about the origin of the funds and the purpose of the business relationship. Obligated entities are also not aware of ML/TF risks arising from their activities.

- An important element of increasing the level of vulnerability is the fact that in the case of unqualified (notifiable) trade, obliged entities do not know that they are an obliged entity and are not aware of the resulting statutory obligations. In most cases, they only fulfil their obligations formally, even if the FSJ sends a notification to such an entity of the performance of inspection.

- General employee awareness of the criminal sanctions is inadequate for most non-financial sector businesses, which means that the threat of criminal sanctions for violations of AML/CTF obligations does not have a sufficiently dissuasive effect.

c) Existence and enforcement of adequate effective and dissuasive sanctions

- In the application of AML/CTF administrative sanctions, the law contains reasonable and dissuasive sanctions, but applicable only to a legal person. However, a vulnerability is their inapplicability to directors, managers or other employees for breach of obligations under the AML/CTF Act.

- A particular vulnerability is the effectiveness of the application of the sanction "initiative to withdraw business license or another trade license". In the case of unqualified (notifiable) trade, the impact of such a sanction is practically nil as the entity can operate independently through several companies without any limitation. Withdrawal of license in one company is a problem for such an obliged entity, and the executive director will move the business to another company with the same sphere of business.

d) Unusual transactions and transaction monitoring

- Insufficient knowledge of AML/CTF issues has a direct impact on UTR monitoring and reporting. From the received UTR reports it can be concluded that their effectiveness is very low. The reason for this is the inability to recognize UTRs and their own determined forms of UTRs⁵².

- In the period under review, the FSJ accepted and inspected a total of 899 UTR reports. Based on the detailed analysis, the following vulnerabilities were identified in UTR monitoring and reporting:

- Inability to recognize UTRs,
- Failure to report follow-up business transactions,
- Failure to verify the origin of funds,

e) Ineffective application of AML/CTF preventive measures

- Inadequate training and knowledge of staff as well as inconsistent compliance with AML/CTF legislation has a direct, but especially adverse, impact on the performance of preventive measures by non-financial sector businesses. In this case, the vulnerability is at a higher level, due in particular to the following facts:

- Inconsistent performance of customer due diligence,
- Possibility to make anonymous deposits to clients,
- Insufficient identification and verification of client identification,
- Insufficient identification and verification of BO identification,
- Insufficient internal control,
- Inefficient activity of the designated person.

- A vulnerability in terms of the practical performance of identifying and verifying the identification of the client (or BO) by non-financial sector businesses is reliance on the information available on the website of the Ministry of Interior SR - lost and stolen documents. In this context, it should be noted that this is a database of previously issued citizens' ID cards and passports, while the false or altered document, which has never been issued by the relevant Slovak state authority, cannot be found in the database of lost and stolen documents.

f) Insufficient application of legislation (control results)

- Strict compliance with the AML/CTF Act and other generally binding legal regulations governing the status, roles and activities of businesses in the non-financial sector is a prerequisite for effective prevention.

- In the period under review, the FSU carried out 61 inspections in the non-financial sector on the basis of a control and analysis plan for the UTR reporting, and the following shortcomings were identified:

- Shortcomings in the programme of own activity of the obliged entity,
- Absence of the programme of own activity of the obliged entity,

⁵² For example, setting a limit of 15,000 EUR for the duty to report, but without any accompanying phenomena and indications that would make it possible to determine that funds could be intended for legalization or terrorist financing.

- Failure to provide FSJ with assistance in carrying out the inspection,
- Non-performance of customer due diligence,

- In the period under review, the Ministry of Finance SR performed 21 inspections of gambling operators. In the event that the inspected obliged entity violated the relevant provisions of the AML/CTF Act, the Ministry of Finance is obliged to refer the said information to FSJ, since it is not entitled to impose sanctions for violating the AML/CTF Act. During the period under review, the Ministry of Finance SR sent the FSJ one piece of information.

g) Unqualified (notifiable) trades

- Significant vulnerability in obtaining business licenses to which the obligations laid down in the AML/CTF Act also apply are unqualified (notifiable) trades. In the case of the non-financial sector, the following entities are affected:

- Organizational and economic advisor,
- Accountant,
- Pawnshop, and
- Legal entity or a natural person authorized to trade in precious metals or gemstones.

- According to the applicable legislation, the only conditions for obtaining unqualified (notifiable) trade license are the applicant's physical age of 18 years and the integrity. No education or experience with company management and bookkeeping is required, which in many cases can lead to unintentional mistakes of negligence or ignorance and, in some cases, to high economic damage. Also, their number is not limited. One owner may have several business companies with the same sphere of business. In the case of unqualified (notifiable) trade, there is no compulsory membership in a professional organization.

- A high level of vulnerability exacerbates the fact that non-financial sector businesses operating unqualified (notifiable) trade often do not know that under the AML/CTF Act they are among obliged entities. The negative consequence is also the absence of a direct flow of information from the FSJ to these obliged entities.

ANALYSIS OF THREATS IN THE SECTOR OF NON-FINANCIAL BUSINESSES AND PROFESSIONS

GENERAL ANALYSIS OF THREATS

a) Legal regulation of the sector of non-financial businesses and professions

- The legislation for individual institutes and the established obligations in the area of prevention of legalization and terrorist financing is primarily included in the AML/CTF Act. It also regulates the obligation to apply a risk-oriented approach to clients. Obligated entities operating in the non-financial sector must have an overview of possible risks associated with a particular client. Based on the information thus obtained, it is mandatory to determine the extent of due diligence and, if necessary, to apply enhanced due diligence.

- General legislation regulates the rights and obligations of individual entities operating in the non-financial sector. In each of the individual categories of the non-financial sector, proof of integrity is required when submitting a license application, a license, a trade license. However, this condition does not apply to employees, which means that not all obliged entities require a proof of integrity from newly recruited employees.

b) Internal AML/CTF policies

- In the case of free legal professions, the function of the designated person is usually performed by a person who obtained a license for the profession. In this case, it is a positive element that such a person has the opportunity to assess the required transaction or business operation from the point of view of AML/CTF at the time when the contract is granted.

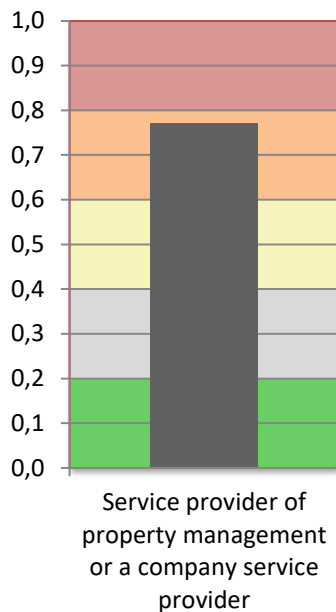
- For professional notifiable trade or unqualified notifiable trade (sphere of business), the function of the designated person is usually performed by the executive director.

- In the period under review, no cases were reported when criminal prosecution against obliged entities, members of their governing bodies or employees for a serious violation of the obligations under the AML/CTF Act, was initiated.

ANALYSIS OF VULNERABILITY OF ENTITIES IN NON-FINANCIAL BUSINESSES AND PROFESSIONS

A. SERVICE PROVIDER OF PROPERTY MANAGEMENT OR A COMPANY SERVICE PROVIDER

On the basis of the evaluation of data and information obtained in connection with the activities carried out by service providers of property management or company service providers, the level of vulnerability was identified at the medium level - a numerical expression of 0.77.



The vulnerability level was adversely affected mainly by :

- Awareness and knowledge of AML/CTF areas,
- Effectiveness of AML/CTF controls,
- Integrity of employees,
- Issue of licenses for business,
- UTR recognition and monitoring,
- Availability and enforceability of sanctions,
- Possibility of establishing an unlimited number of companies which are subsequently provided free of charge to other owners to whom services are provided subsequently at the price at which the change of the owner is offset,
- Non-transparent performance of the activity (without proper trade license).

The said sphere of business (service providers of property management or company service providers) is not included in the Trades Licensing Act. These actions are performed under the following licenses for:

- Rental of real property associated with the provision of other than basic services related to rental,
- Organizational and economic consulting,
- Bookkeeping, or
- Administrative services.

In the period under review, the FSJ performed 3 on-site inspections and found shortcomings in the programme of own activities. Monetary sanctions were imposed for violations of the AML/CTF Act.

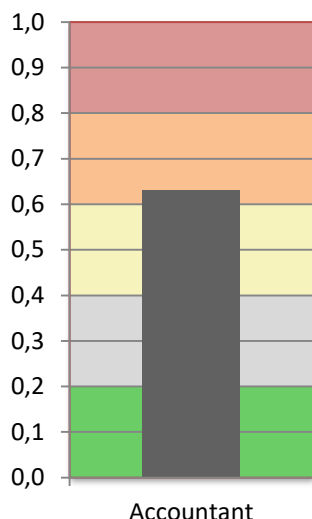
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
3.	Integrity of employees
4.	Effectiveness of UTR reporting and monitoring
5.	Availability and enforceability of input controls
6.	Effectiveness of compliance function (organization)
7.	Availability and enforcement of criminal sanctions
8.	Availability of credible infrastructure for identification
9.	Availability and access to BO information
10.	Availability of independent information sources

B. ACCOUNTANT

On the basis of the evaluation of data and information obtained in connection with the activities carried out by accountants, the level of vulnerability was identified at the medium-high level - a numerical expression 0.63.



The vulnerability level was adversely affected mainly by:

- Conditions for issuing an unqualified (notifiable) trade license,
- Possibility of setting up an unlimited number of companies, in the case of withdrawal of the business license in one company, the natural person or the legal entity may continue to provide that activity through another company with the same activity with the same sphere of business,
- Effectiveness of AML/CTF control,
- Knowledge and awareness of AML/CTF area and ML/TF risks related to the sphere of business,
- No internal control,
- Limited possibilities to ensure the flow of information regarding AML/CTF,
- No use of the possibility of exchanging information between obliged entities in accordance with the relevant provisions of AML/CTF Act,
- Failure to keep written documents of business in accordance with the relevant provisions of AML/CTF Act.

An accountant carries out his activity on the basis of unqualified (notifiable) trade license issued by the relevant district office - the Trade Licensing Department. It is not necessary to prove the relevant education or experience in accounting to get an unqualified (notifiable) trade license as an accountant. This can lead to unintentional errors, which can result in tax crime.

In the period under review, FSJ carried out a total of 8 on-site inspections, while shortcomings were found in the programme of its own activity or due to an absence of a programme of own activity. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ received and verified a total of 5 UTR reports.

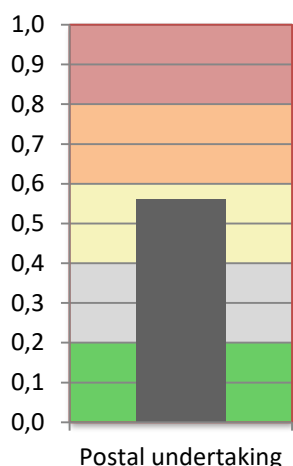
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Availability and enforceability of input controls
2.	Effectiveness of supervision and control activities
4.	Effectiveness of compliance function (organization)
5.	Availability and enforcement of administrative sanctions
6.	Integrity of employees
7.	Effectiveness of UTR reporting and monitoring
8.	Availability and enforcement of criminal sanctions
9.	Availability of credible infrastructure for identification
10.	Availability and access to BO information
11.	Availability of independent information sources

C. POSTAL UNDERTAKING

On the basis of the evaluation of data and information obtained in connection with the activities carried out by postal undertakings, the level of vulnerability was identified at the medium level - a numerical expression 0.56.



The vulnerability level was adversely affected mainly by:

- Possibility of making cash payments,
- Diversity of activities carried out,
- Acting as an intermediary for other obliged entities,
- Absence of AML/CTF controls,
- Effectiveness of the activity of the designated person,
- Low efficiency of UTR reporting - UTR recognition,
- Insufficient professional training,
- Failure to implement customer due diligence measures.

The postal undertaking operates under a license issued by the Regulatory Authority for Electronic Communications and Postal Services.

In the period under review, FSJ carried out no AML/CTF control.

In the period under review, FSJ received and verified a total of 579 UTR reports.

Determination of priorities in activities of relevant bodies:

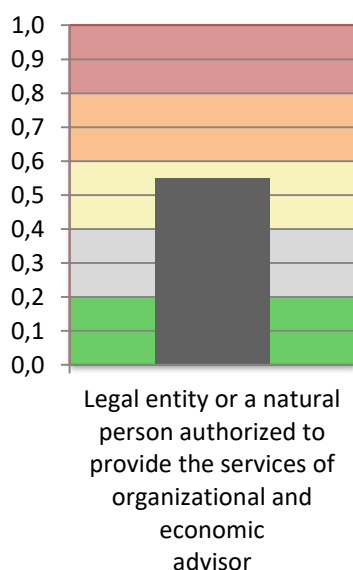
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of supervision and control activities
2.	Effectiveness of compliance function (organization)

2.	Effectiveness of UTR reporting and monitoring
4.	Availability and enforcement of criminal sanctions
5.	Availability of credible infrastructure for identification
6.	Availability and access to BO information
7.	Availability of independent information sources

D. LEGAL ENTITY OR A NATURAL PERSON AUTHORIZED TO PROVIDE THE SERVICES OF ORGANIZATIONAL AND ECONOMIC ADVISOR

On the basis of the evaluation of data and information obtained in connection with the activities carried out by legal entities or natural persons authorized to provide the services of organizational and economic advisor, the level of vulnerability was identified at the medium level - a numerical expression 0.55.



The vulnerability level was adversely affected mainly by:

- Insufficient effectiveness of AML/CTF control,
- Availability and enforceability of sanctions,
- Issue of business licenses,
- The possibility of sophisticated assisting in the commission of ML, especially when establishing a company, providing a registered office linked to the provision of services to business companies and accountants,
- Knowledge and awareness of AML/CTF area and ML/TF risks related to the sphere of business,

- Effectiveness of the activity of the designated person,
- Low efficiency of UTR reporting - UTR recognition and monitoring,
- Impossibility of online verification of BO information,
- Possibility of having an unlimited number of companies with this sphere of business and subsequently transferring it to other persons, often to foreign persons (in the proposal to withdraw the license, the possibility of doing so through another company),
- Possibility of establishing an unlimited number of companies which are subsequently provided free of charge to other owners to whom services are provided subsequently for trade companies,
- Performance of legal services - the establishment of companies, through a contract lawyer or a notary, to whom services are provided subsequently for trade companies.

Legal entities or natural persons authorized to provide the services of organizational and economic advisor carry out his activity on the basis of unqualified (notifiable) trade license issued by the relevant district office - the Trade Licensing Department. No education or experience in company management is required.

In the period under review, FSJ carried out a total of 17 on-site inspections, while shortcomings were found in the programme of its own activity or due to an absence of a programme of own activity, non-performance of customer due diligence. A serious shortcoming was the failure to allow the performance of inspection. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ received and verified a total of 10 UTR reports.

Determination of priorities in activities of relevant bodies:

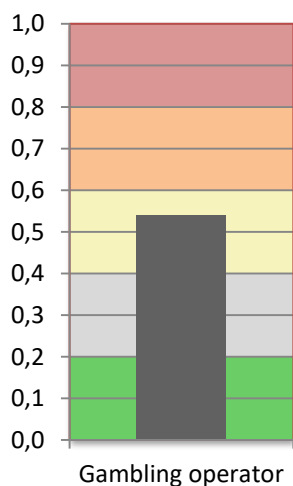
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
2.	Availability and enforceability of input controls
4.	Effectiveness of compliance function (organization)
5.	Availability and enforcement of criminal sanctions
6.	Availability and enforcement of administrative sanctions

7.	Effectiveness of UTR reporting and monitoring
8.	Integrity of employees
9.	Availability of credible infrastructure for identification
10.	Availability and access to BO information
11.	Availability of independent information sources

E. GAMBLING OPERATOR

On the basis of the evaluation of data and information obtained in connection with the activities carried out by gambling operators, the level of vulnerability was identified at the medium level - a numerical expression 0.54.



The vulnerability level was adversely affected mainly by:

- Low number of inspections by FSJ and MF SR,
- Insufficient training programs, resulting in ignorance of AML Act,
- Failure to perform enhanced customer due diligence if the client is not physically present at the obliged entity (betting offices, Internet games),
- Failure to perform customer due diligence if gambling is performed outside gambling clubs and casinos, the so-called „mediator“,
- Impossibility to monitor each other's follow-up operations aimed at reaching the limit of EUR 15,000 if there is no business relationship with the client, anonymous deposits - the possibility of misuse of winning tickets to other persons, which makes it possible to legalize the FP (Internet offer),
- Insufficient internal control,

- Insufficient availability and enforceability of sanctions,
- Insufficient availability of independent information sources,
- Cash payments.

The gambling operator runs a business under a license issued by the Ministry of Finance SR.

In the period under review, FSJ carried out a total of 5 on-site inspections, while shortcomings were found in the programme of its own activity, non-performance of customer due diligence and impossibility to monitor each other's follow-up operations. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, the Ministry of Finance SR carried out a total of 21 on-site inspections, while shortcomings found in one case were referred to FSJ.

In the period under review, FSJ received and verified a total of 168 UTR reports.

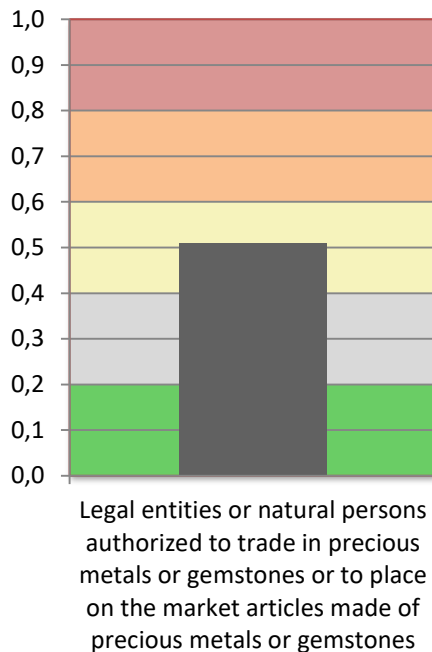
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
2.	Effectiveness of compliance function (organization)
4.	Availability and enforcement of criminal sanctions
5.	Effectiveness of UTR reporting and monitoring
6.	Availability of credible infrastructure for identification
7.	Availability of independent information sources

F. LEGAL ENTITY OR A NATURAL PERSON AUTHORIZED TO TRADE IN PRECIOUS METALS OR GEMSTONES, AND TO PLACE ON THE MARKET ARTICLES MADE OF PRECIOUS METALS OR GEMSTONES

On the basis of the evaluation of data and information obtained in connection with the activities carried out by legal entities or natural persons authorized to trade in precious metals or gemstones or to place on the market articles made of precious metals or gemstones, the level of vulnerability was identified at the medium level - a numerical expression 0.51.



The vulnerability level was adversely affected mainly by:

- Compliance effectiveness,
- Effectiveness of supervision,
- Input control mechanisms - unqualified (notifiable) trade license that can be obtained without adequate education,
- Non-transparency in the sphere of business in the Trade Register or in the Commercial Register.

Legal entities or natural persons authorized to trade in precious metals or gemstones or to place on the market articles made of precious metals or gemstones run a business under unqualified (notifiable) trade license, which is issued by the relevant district office - the Trade Licensing Department. However, the business can be performed under the sphere of business a) trading in precious metals, gemstones; b) purchase and sale of goods (retail and wholesale). The Assay Act establishes the obligation to register traders who are actually engaged in trade in precious metals and gemstones. In the event of failure to comply with this obligation, their business authorization is not affected.

In the period under review, FSJ carried out a total of 4 on-site inspections, while shortcomings were found in the programme of its own activity, non-performance of customer due diligence. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ received and verified no UTR report.

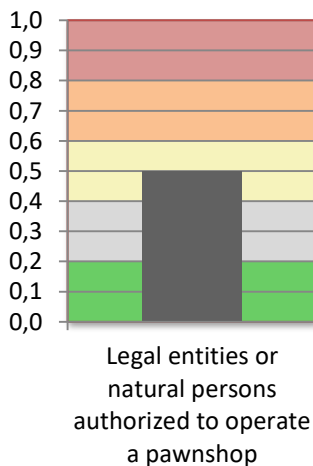
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of compliance function (organization)
2.	Effectiveness of supervision and control activities
2.	Availability and enforceability of input controls
4.	Effectiveness of UTR reporting and monitoring
5.	Availability and enforcement of criminal sanctions
6.	Availability of credible infrastructure for identification
7.	Availability of independent information sources

G. LEGAL ENTITY OR A NATURAL PERSON AUTHORIZED TO OPERATE A PAWNSHOP

On the basis of the evaluation of data and information obtained in connection with the activities carried out by legal entities or natural persons authorized to operate a pawnshop, the level of vulnerability was identified at the medium level - a numerical expression 0.50.



The vulnerability level was adversely affected mainly by:

- Unqualified (notifiable) trade license that can be obtained without any education,
- Entrepreneurs do not know that they are obliged entities,
- Ignorance of AML duties, (non-identification of the origin of property),
- Effectiveness of supervision,
- Effectiveness of compliance functions,
- Availability of input controls,
- Effectiveness of UTR monitoring,

Legal entities or natural persons authorized to operate a pawnshop run a business under unqualified (notifiable) trade license, which is issued by the relevant district office - the Trade Licensing Department.

In the period under review, FSJ carried out a total of 4 on-site inspections, while shortcomings were found in the programme of its own activity. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ received and verified no UTR report.

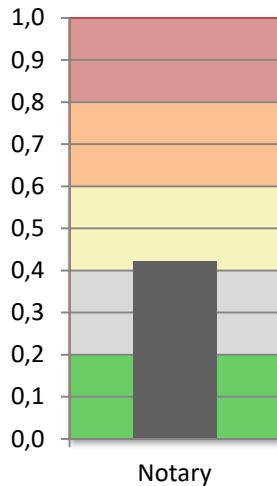
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
2.	Effectiveness of compliance function (organization)
4.	Availability and enforceability of input controls
5.	Effectiveness of UTR reporting and monitoring
6.	Availability and enforcement of administrative sanctions
7.	Availability and enforcement of criminal sanctions
8.	Availability of credible infrastructure for identification
9.	Availability of independent information sources

H. NOTARY

On the basis of the evaluation of data and information obtained in connection with the activities carried out by notaries, the level of vulnerability was identified at the medium level - a numerical expression 0.47.



The vulnerability level was adversely affected mainly by:

- Insufficient supervision effectiveness, supported by the low number of controls carried out, guidelines and published information on the forms and methods of legalization and ways of recognizing UTRs by FSJ,
- Poor availability and enforceability of criminal sanctions for legalization,
- Poor performance of AML compliance function (non-acceptance of disciplinary measures for non-compliance with AML duties towards employees, insufficient internal control),
- Impossibility of online verification of BO information,
- Not paying attention to the value of the legal service provided (origin of assets and funds - KYC),
- Possibility of a cash deposit for safekeeping and auctioning, where notaries see the potential risk of money laundering,
- Non-use of the possibility of providing information under Article 18 par. 8 b) and c).

The notary carries out his activities on the basis of registration in the Chamber of Notaries of Slovak Republic. The notary is appointed by the Minister of Justice of the SR. The obliged entity is a notary who provides the client with a legal service related to:

- Purchase and sale of real estate or business shares in a company,
- Administration or safekeeping of funds, securities or other assets,
- Opening or managing an account with a bank or branch of a foreign bank or securities account,
- Establishment, activity or management of a company, association of natural persons and legal persons, special-purpose association of assets or another legal person.

In the period under review, FSJ carried out a total of 2 on-site inspections, while shortcomings were found in the programme of its own activity. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ received and verified a total of 21 UTR reports.

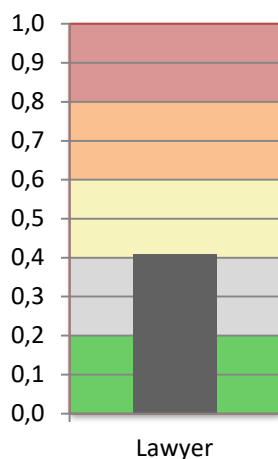
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of compliance function (organization)
2.	Availability and enforcement of criminal sanctions
4.	Effectiveness of supervision and control activities
5.	Effectiveness of UTR reporting and monitoring
6.	Availability and access to BO information

I. LAWYER

On the basis of the evaluation of data and information obtained in connection with the activities carried out by lawyers, the level of vulnerability was identified at the medium level - a numerical expression 0.41.



The vulnerability level was adversely affected mainly by:

- Insufficient supervision effectiveness, supported by the low number of controls carried out, guidelines and published information on the forms and methods of legalization and ways of recognizing UTRs by FSJ,
- Poor or insufficient understanding of the risks of the profession in relation to the possibilities of money laundering - (not paying attention to the value of the legal service provided, the origin of assets and funds - KYC, since funds does not pass through a lawyer's account),
- Poor availability and enforceability of criminal sanctions for legalization,
- Poor performance of the AML compliance,
- Failure to take measures for failure to comply with AML duties towards employees, insufficient of internal control,
- Effectiveness of the UTR reporting,
- Absence of public national registers, impossibility of online verification of BO information,
- Non-use of the possibility of providing information under Article 18 par. 8 b) and c) of Act No. 297/2008 Coll.

The lawyer carries out his activities on the basis of registration in the Slovak Bar Association. The obliged entity is a lawyer who provides the client with a legal service related to:

- Purchase and sale of real estate or business shares in a company,
- Administration or safekeeping of funds, securities or other assets,
- Opening or managing an account with a bank or branch of a foreign bank or securities account,
- Establishment, activity or management of a company, association of natural persons and legal persons, special-purpose association of assets or another legal person.

In the period under review, FSJ carried out a total of 6 on-site inspections, while shortcomings were found in the programme of its own activity, non-performance of cooperation during inspection. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ received and verified a total of 10 UTR reports.

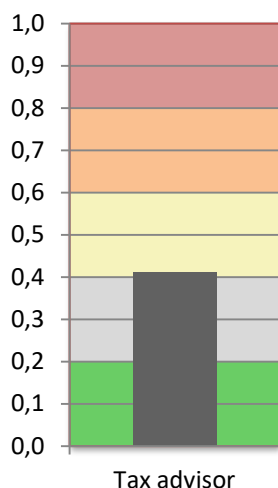
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of supervision and control activities
2.	AML awareness of employees
2.	Effectiveness of compliance function (organization)
4.	Effectiveness of UTR reporting and monitoring
5.	Availability and enforcement of criminal sanctions
6.	Availability of credible infrastructure for identification
7.	Availability and access to BO information
8.	Availability of independent information sources

J. TAX ADVISOR

On the basis of the evaluation of data and information obtained in connection with the activities carried out by tax advisors, the level of vulnerability was identified at the medium level - a numerical expression 0.41.



The vulnerability level was adversely affected mainly by:

- Effectiveness of supervision,
- Availability of enforcement of criminal sanctions,
- Ignorance of AML in business,
- Availability and enforceability of criminal sanctions,
- Impossibility of online verification of BO information,
- Not paying attention to the value of the service provided, since funds does not pass through a tax advisor's account,
- Non-use of the possibility of providing information under Article 18 par. 8 b) and c) of Act No. 297/2008 Coll.

The tax advisor performs his activity on the basis of a license issued by the Slovak Chamber of Tax Advisors, membership in the Chamber is compulsory. The MF SR is the supervisory body.

In the period under review, FSJ carried out a total of 1 on-site inspection, while shortcomings were found in the programme of its own activity. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ received and verified a total of 5 UTR reports.

Determination of priorities in activities of relevant bodies:

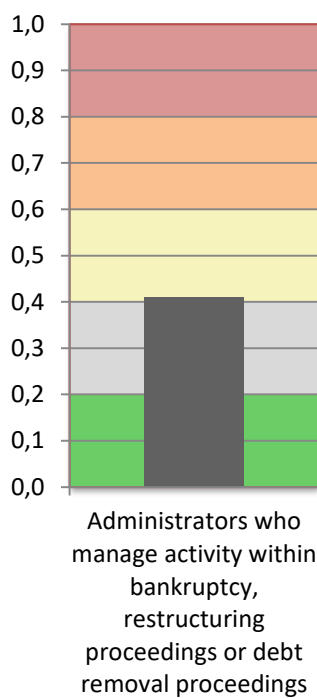
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of supervision and control activities

2.	AML awareness of employees
2.	Availability and enforcement of criminal sanctions
4.	Availability of credible infrastructure for identification
5.	Availability and access to BO information
6.	Availability of independent information sources

K. ADMINISTRATOR WHO MANAGES ACTIVITY WITHIN BANKRUPTCY, RESTRUCTURING PROCEEDINGS OR DEBT REMOVAL PROCEEDINGS

On the basis of the evaluation of data and information obtained in connection with the activities carried out by administrators who manage activity within bankruptcy, restructuring proceedings or debt removal proceedings, the level of vulnerability was identified at the medium level - a numerical expression 0.41.



The vulnerability level was adversely affected mainly by:

- Insufficient effectiveness of supervision (zero controls performed),
- Availability and enforceability of criminal sanctions,
- Obligation to accept cash payment at auction,
- insufficient knowledge of AML - the content of the state examination is not AML,
- Effectiveness of compliance function – executive officer.

The administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings performs his activity on the basis of registration in the List of Administrators. The Ministry of Justice S SR decides on registration and deletion and suspension of the activities of the administrator. At the same time, the Ministry of Justice of the Slovak Republic is the supervisory authority over the performance of administrative activities.

In the period under review, FSJ carried out no on-site inspection.

In the period under review, FSJ received and verified no UTR report.

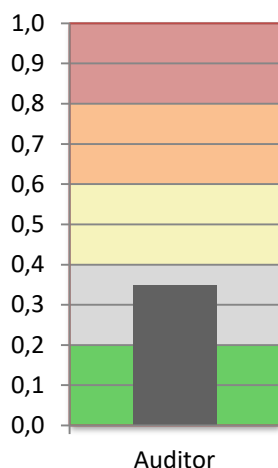
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of supervision and control activities
2.	AML awareness of employees
2.	Effectiveness of compliance function (organization)
4.	Availability and enforcement of criminal sanctions
5.	Availability of credible infrastructure for identification

L. AUDITOR

On the basis of the evaluation of data and information obtained in connection with the activities carried out by auditors, the level of vulnerability was identified at the medium-low level - a numerical expression 0.35.



The vulnerability level was adversely affected mainly by:

- Availability and enforceability of criminal sanctions,
- Availability and reliability of the identification infrastructure,
- Availability of independent information sources,
- No use of the possibility of exchanging information under Article 18 par. 8 b) and c) of Act No. 297/2008 Coll.

The auditor performs his activity on the basis of a license issued by the Audit Oversight Office, which is also the supervisor of the performance of audit activities.

In the period under review, FSJ carried out 1 on-site inspection, whereas shortcomings in the programme of own activity were found and non-performance of the obligation to perform customer due diligence. Monetary sanctions were imposed for violations of the AML/CTF Act.

In the period under review, FSJ imposed monetary sanctions and verified a total of 7 UTR reports.

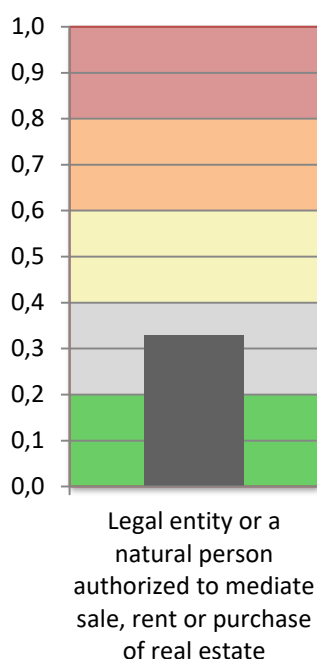
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Availability and enforcement of criminal sanctions
2.	Availability of credible infrastructure for identification
2.	Availability of independent information sources

M. LEGAL ENTITY OR A NATURAL PERSON AUTHORIZED TO MEDIATE SALE, RENT OR PURCHASE OF REAL ESTATE

On the basis of the evaluation of data and information obtained in connection with the activities carried out by legal entities or natural persons authorized to mediate sale, rent or purchase of real estate, the level of vulnerability was identified at the medium-low level - a numerical expression 0.33.



The vulnerability level was adversely affected mainly by:

- Supervision effectiveness,
- Poor awareness of AML obligations,
- Effectiveness of the responsible person for legalization,
- Availability and enforceability of criminal sanctions,
- Not paying attention to the value of the property from the point of view of AML, as funds usually do not pass through the account of the real estate agency (origin, KYC),
- Entrepreneurs who obtain this authorization do not know that they are obliged persons under Act no. 297/2008 Coll.

Legal entities or natural persons authorized to operate mediate sale, rent or purchase of real estate, run a business under professional notifiable trade license, which is issued by the relevant district office - the Trade Licensing Department. The condition for obtaining a professional notifiable trade license is a university degree in economics, construction, architectural or legal specialization or secondary education with a school-leaving

examination and 5 years of experience in the field. Professional organization membership is not compulsory.

In the period under review, FSJ carried out 8 on-site inspections, whereas shortcomings in the programme of own activity were found. In two cases, an obliged entity did not allow the FSJ inspection. Monetary sanctions were imposed for violations of the AML/CTF Act and a motion was filed to withdraw a license for business or other self-employed activities.

In the period under review, FSJ received and verified a total of 90 UTR reports.

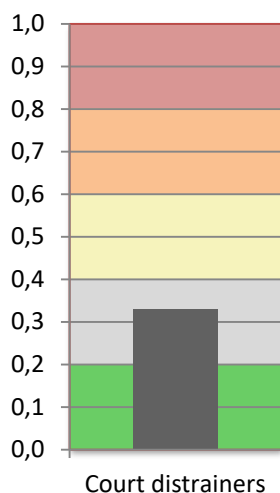
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
2.	Effectiveness of compliance function (organization)
4.	Availability and enforcement of criminal sanctions
5.	Availability of credible infrastructure for identification
6.	Availability and access to BO information
7.	Availability of independent information sources

N. COURT DISTRAINER

On the basis of the evaluation of data and information obtained in connection with the activities carried out by court distrainers, the level of vulnerability was identified at the medium-low level - a numerical expression 0.33.



The vulnerability level was adversely affected mainly by:

- Insufficient supervision effectiveness, supported by the low number of controls carried out, guidelines and published information on the forms and methods of legalization and ways of recognizing UTRs by FSJ,
- Possibility of receiving a cash payment at auction,
- Poor availability and enforceability of criminal sanctions for legalization,

The court distrainer performs his activity on the basis of entry in the list of distrainers. Ministry of Justice SR appoints and dismisses court distrainers and keeps the list. Membership in the Slovak Chamber of Executors is mandatory.

In the period under review, FSJ carried out 2 on-site inspections, no shortcomings were found.

In the period under review, FSJ received and verified a total of 2 UTR reports.

Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the non-financial sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Availability and enforcement of criminal sanctions
2.	Effectiveness of supervision and control activities

2.3. OTHER FINANCIAL INSTITUTIONS SECTOR

GENERAL INFORMATION ON THE SECTOR OF OTHER FINANCIAL INSTITUTIONS IN THE SLOVAK REPUBLIC

The OFI sector has long been an expanding segment of the Slovak national economy. The competent authorities of the SR have precise information on the number of issued licenses for the activities of individual OFI categories. Given the number of licenses issued, we classify the sector in question as a large sector. In accordance with the legal definition of the obliged entity resulting from the AML/CTF Act, we distinguished 8 individual categories of OFI:

- i) a commodity exchange,
- ii) a financial agent, financial advisor,
- iii) a legal person or a natural person authorized to carry out an exchange activity - exchange office,
- iv) a legal person or a natural person authorized to sell accounts receivable - factoring,
- v) a legal entity or a natural person authorized to carry out auctions out of distraintments,
- vi) finance lease or other financial services under a special regulation - leasing,
- vii) a payment institution, a payment service agent and an electronic money institution, and
- viii) creditor.

An overview of issued licenses for performing a financial institution other than a bank in the period under review:

Obliged entity/year	2010	2011	2012	2013	2014	2015
Commodity exchange	1	1	1	1	1	1
Fin. agent	47089	33639	34487	34196	34098	34100
Fin. advisor	15	21	15	15	13	12
Factoring	30301	31411	32813	33701	48096	48358
Creditor	26	26	26	25	25	26
Leasing	16815	17473	18496	28268	42058	41701
PI/PSA/EMI	1/0/0	4/2/0	5/2/0	7/2/0	8/2/0	9/2/1
Auction	598	650	683	667	1194	1238
Exchange office	2480	2491	2503	2512	2519	2525

A negative phenomenon accompanying the statistics on the number of licenses issued is the fact that there is no information and statistical data on the number of entities actually performing this activity. This applies in particular to the following OFI categories:

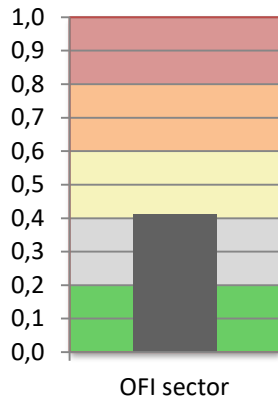
- factoring,

- leasing,
- auction, and
- exchange offices.

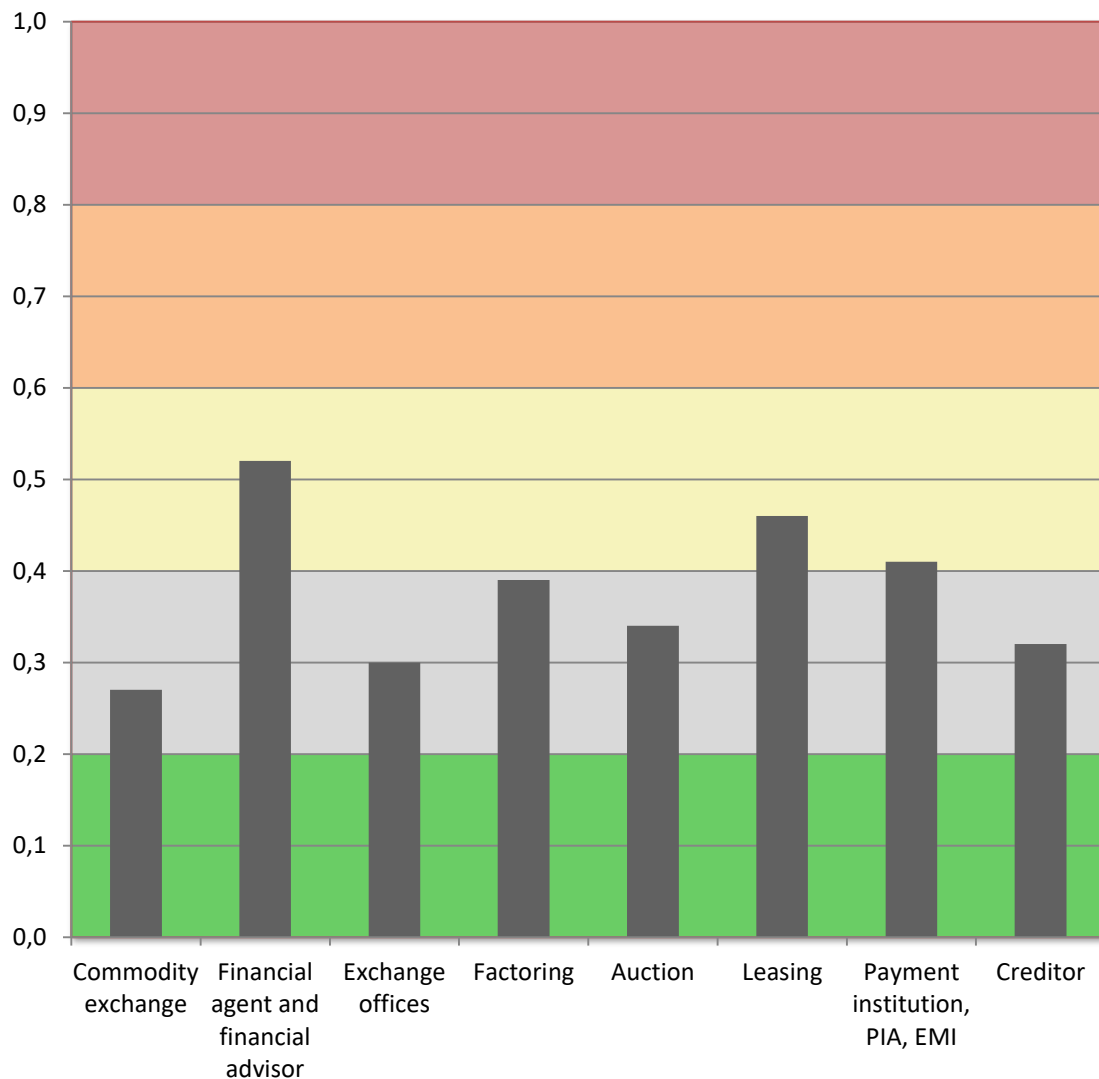
In general, the high total number of entities in the OFI sector, as well as the unclear number of genuine operating entities, result in a high level of vulnerability in terms of communication, issuing guidelines and notifications in relation to FSJ or the NBS. It is also a vulnerability in terms of performance of control or supervision.

VULNERABILITY OF THE SECTOR OF OTHER FINANCIAL INSTITUTIONS

The overall vulnerability of the OFI sector in the Slovak Republic was based on the evaluation of the collected information and data at the medium level, a numerical expression of the overall level of vulnerability at 0.41 – please see the graph.



Comparative graph of the vulnerability levels of individual entities of the sector Other financial institutions



The following facts were considered in the analysis of the OFI sector:

- Total size / volume of OFI category,
- Category profile based on client,
- Use of agents,
- Level of cash activity,
- Frequency of international transactions, and
- Other (anonymous use of products, detection of transaction records, existence of ML typology, use of products without physical presence of the client, abuse of OFI for committing tax crime and fraud).

PROCEDURAL VULNERABILITY

VULNERABILITIES IN THE SECTOR OF OTHER FINANCIAL INSTITUTIONS

The following vulnerabilities were identified by assessing the procedural aspect related to the performance of the activities and internal processes of the individual entities of the sector Other financial institutions businesses as well as the supervisory and control bodies:

- Average knowledge of the laws, principles and procedures in the fight against AML/CTF by both employees and the obliged entity,
- Absence of awareness of the fact that OFIs are obliged entities and the resulting obligations,
- Unclear number of entities actually operating in the OFI sector,
- Absence of authorization for AML/CTF supervision for NBS staff performing foreign exchange supervision,
- Absence of methodological guidance on compliance with ML/TF legislation on prevention for individual categories of OFIs,
- Absence of joint inspections of FSJ and NBS in order to develop mutual cooperation and exchange of experience,
- Low number of FSJ staff and the low number of inspections carried out in proportion to the number of obliged entities in the OFI sector, and
- Absence of remote control, despite legal authorization.

Detailed analysis of selected vulnerabilities in the sector of Other financial institutions

a) Insufficient knowledge and awareness of the ML/TF risks and their management

- Shortcomings in professional staff training and employee verification are a significant vulnerability that has a direct impact on the performance of other activities of OFI entities. Although the AML/CTF Act imposes the obligation to undertake training of employees on the commencement of employment and subsequently once a year, most entities have assessed their employees' knowledge as average. A negative phenomenon in the education of employees of these entities is also the absence of knowledge verification.

- Clearly the most vulnerable place that the evaluation process revealed was the fact that not all entities operating in the OFI sector or natural persons who control and manage these entities are aware that they are considered obliged entities under the AML/CTF Act⁵³.

- Insufficient and ineffective methodological and training activities performed by the NBS and FSJ can also be considered as a vulnerable place in this area.

b) Insufficient application of legislation (inspection results)

⁵³ Despite the fact that the principle of "ignorantia iuris non excusat" is applied in the conditions of the SR, the competent authorities should not be relieved of their responsibility to provide adequate information on possible other obligations of business entities arising from special regulations when issuing business licenses.

- Consistent compliance with AML/CTF Act and other generally binding legal regulations governing the status, roles and activities of entities in the OFI sector is a prerequisite for effective prevention.

In the period under review, the NBS carried out a total of 40 supervisory inspections in the OFI sector (specifically in the categories of financial agent / financial advisor; legal entity or natural person authorized to carry out exchange activities – exchange office; creditor and payment institution / payment agent / electronic money institution), almost no shortcomings were identified. The only shortcoming found was that an obliged entity did not have AML/CTF activities regulated by the Articles of Association.

In the period under review, the FSJ carried out a total of 57 inspections in the OFI sector on the basis of the control plan and analyses of UTR reports, with the following shortcomings found:

- Shortcomings in the obliged entity's own activity programme,
- Absence of own activity programme,
- Insufficient client identification,
- Failure to identify the client,
- Shortcomings in the adoption of CDD measures,
- CDD not performed,
- Entity was unaware that they were an obliged entity,
- Absence of staff training,
- Failure to provide FSJ with assistance during inspection.

c) ineffectiveness of control and supervision in the AML/CTF area

- In particular, insufficient staffing, technical and financial resources at FSJ are the vulnerability in the field of inspection of the OFI sector. As in the case of obliged entities, the absence of continuous training and the acquisition of the necessary skills and experience persists in the case of control authorities. This vulnerability is also exacerbated by a very clear disproportion between the number of FSJ officers responsible for enforcement and the number of obliged entities only in the OFI sector. In the period under review, the numerical expression of the ratio (or disproportion) is on average 5:127 972. The absence of remote control may also be considered as vulnerability. Although the AML/CTF Act allows this type of control, it is not used in application practice.

- Two vulnerabilities can be identified in terms of NBS supervision over relevant OFI entities. As in the case of FSJ, in the case of the NBS, it is also necessary to increase the staff number for AML / CTF supervision. A particular vulnerability in the supervision in exchange offices is the absence of authorization in the so-called Foreign exchange law for competent supervisory authorities to implement thematic AML/CTF supervision. This fact, based on the principle of "cascading effect", has a significant adverse impact on staffing capacities, training, methodology and cooperation with other competent authorities at national and international level.

- Vulnerability affecting the performance of inspections by the FSJ and the supervision by the NBS is also the absence of mutual cooperation, exchange of information and performance of

joint controls. During the period under review, no joint control of any of the entities operating in the OFI sector was recorded.

d) Ineffective application of AML/CTF preventive measures

- Inadequate training and knowledge of staff as well as inconsistent compliance with AML / CTF legislation has a direct but especially adverse impact on the performance of preventive measures by obliged entities. In this case, the vulnerability is at a higher level, due to the following facts:

- Inconsistent adoption of client identification measures,
- Inconsistent performance of CDD
- Sorting and categorizing clients according to their risk level.

- The increased vulnerability potential also has the absence of methodological guidance for entities active in the OFI sector for performance of their obligations under the legislation to prevent ML and TF for each category. In particular, the methods and forms of legalization are noticeably absent. From the point of view of the division of responsibilities, this is a vulnerability in the area of competence of the FSJ as well as the NBS.

- One of the effective tools, which is markedly absent in the OFI sector, is the regular performance of an audit aimed at assessing the effectiveness of AML/CTF compliance measures.

e) Unusual transactions and transaction monitoring

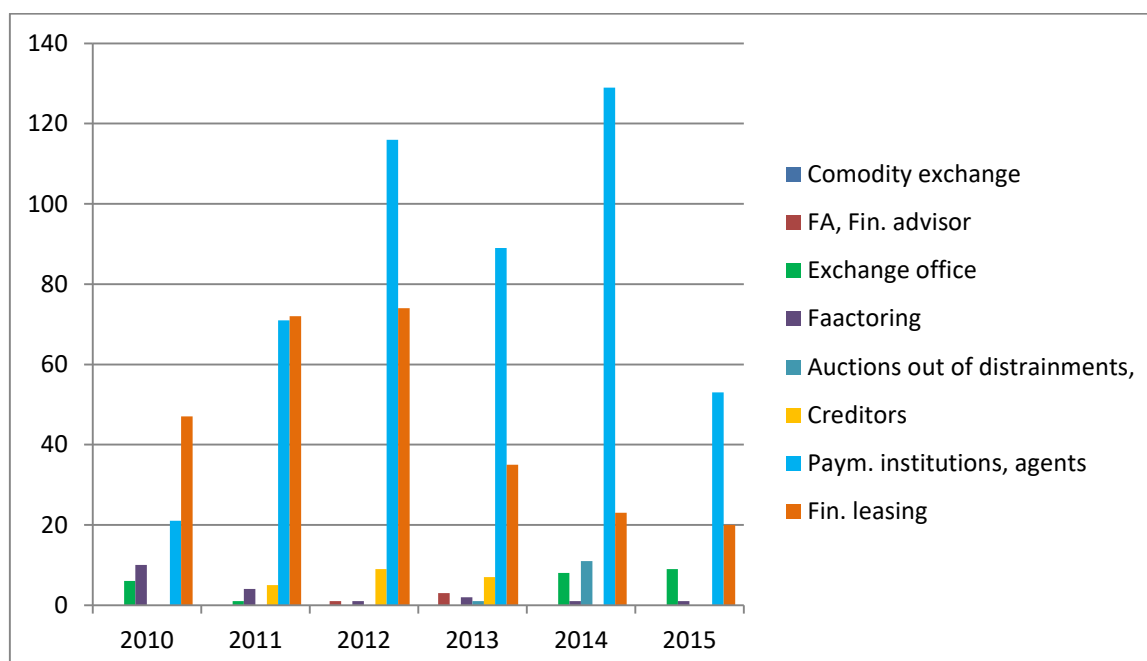
- The vulnerability from the organizational and technical point of view for legal obligations, in particular in relation to monitoring transactions and clients, and the subsequent reporting is in particular the fact that the vast majority of OFI entities use a manual AML/CTF monitoring system to identify unusual transactions. The same part of these entities uses manual systems to control new and existing clients, whether they are on the list of sanctioned persons, or whether they are PEPs. In particular, payment institutions use automated monitoring systems.

In the period under review, FSJ received and verified a total of 837 UTR reports. Based on a detailed analysis, the following vulnerabilities in UTR monitoring and reporting were identified:

- Non-verification of the origin of funds,
- Insufficient implementation of due diligence by financial institutions that mediate payments to entities operating in the OFI sector,
- Absence of exchange of information between obliged entities,
- Ignorance of potential methods and forms of legalization related to individual OFI categories.

The highest number of received UTRs was in the category of payment institutions and payment service agent, i.e. entities that provide products based on cash or international cashless transfers, see the table and the graph.

Obligated entity/year	2010	2011	2012	2013	2014	2015
Commodity exchange	0	0	0	0	0	0
FA and Fin. advisor	0	0	1	3	0	0
Exchange office	6	1	1	0	8	9
Factoring	10	4	1	2	1	1
Creditors	0	5	9	7	11	0
PI/PSA/EMI	21	71	116	89	136	52
Auction	0	0	0	1	0	0
Leasing	47	72	74	35	23	20



ANALYSIS OF THREATS OF THE SECTOR OF OTHER FINANCIAL INSTITUTIONS

GENERAL ANALYSIS OF THREATS

a) Legal regulation of the sector of other financial institutions

The legislation for individual institutes and the established obligations in the area of prevention of legalization and terrorist financing is primarily included in the AML/CTF Act. It also regulates the obligation to apply a risk-oriented approach to clients. Obligated entities operating in the OFI sector must have an overview of possible risks associated with a particular client. Based on the information thus obtained, it is mandatory to determine the extent of due diligence and, if necessary, to apply enhanced due diligence.

General legislation regulates the rights and obligations of individual entities operating in the OFI sector. In each of the individual categories of the OFI sector, proof of integrity is required when submitting a license application, a license, a trade license. However, this condition does not apply to employees, which means that not all obliged entities require a proof of integrity from newly recruited employees⁵⁴.

b) Internal AML/CTF policies

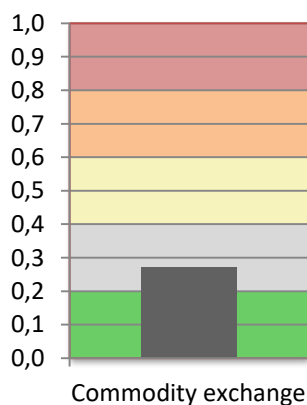
- The structure of entities operating in the OFI sector is diverse. Most people with a minimum number of employees (one to two) prevail. On the opposite side of the spectrum, there are entities consisting of branches located throughout Slovakia. This fact, together with the sphere of business and the structure of the products and services provided, has a direct impact on the organizational and staffing of the AML / CTF measures within the entity's internal organizational structure, the system of client risk assessment and the company's monitoring system designed to identify UTRs. On the basis of the available information, larger entities provide the designated persons with independence in decision making. For other entities, the activity of the designated person is provided by a statutory representative, as these are entities with a small number of employees.

In the period under review, no violations in the AML / CTF area by employees of the entities operating in the OFI sector were reported.

ANALYSIS OF VULNERABILITY OF INDIVIDUAL ENTITIES IN THE SECTOR OF OTHER FINANCIAL INSTITUTIONS

A. COMMODITY EXCHANGE

On the basis of the evaluation of data and information obtained in connection with the activities carried out by commodity exchanges, the level of vulnerability was identified at the medium-low level - a numerical expression 0.27.



⁵⁴ In the period under review, two cases of breach of integrity were recorded by an employee in one of the payment institutions operating in the Slovak Republic. In both cases, the payment institution terminated the employment.

The general legislation⁵⁵ regulates the status and roles of the stock exchange so that it operates as a safe and transparent regulated market for various commodities, excluding weapons and poisons. At the end of the period under review, there was one commodity exchange on the territory of the SR, which had approximately 20 direct members. Transactions are carried out through stock exchange brokers without the personal participation of the Exchange members. Funds such as remuneration for commodities that the law allows to buy and sell through a commodity exchange are transferred only by cashless transfer. The share of international transactions is low, as a large majority of members are trade companies based in Slovakia⁵⁶.

The general supervision of the commodity exchange activity is carried out by the so-called stock exchange commissioner. The performance of AML / CTF control measures is performed exclusively by FSJ.

The level of vulnerability is adversely affected by the use of this service without the personal participation of Exchange members.

Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

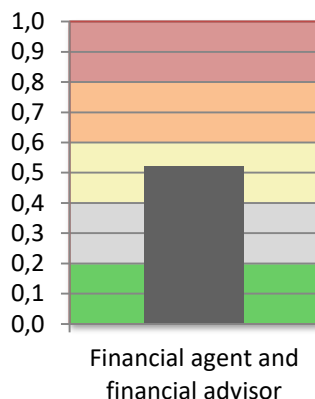
Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
3.	Effectiveness of UTR reporting and monitoring
4.	Availability and enforcement of criminal sanctions
5.	Effectiveness of compliance function (organization)
6.	Availability and access to BO information
7.	Availability and enforcement of administrative sanctions
8.	Availability of independent information sources

⁵⁵ Act No. 92/2008 Coll. on Commodity Exchanges, as amended

⁵⁶ A natural person may also be a member of a commodity exchange, but no such person is currently a member of the Exchange in Slovakia

B. FINANCIAL AGENT AND FINANCIAL ADVISOR

On the basis of the evaluation of data and information obtained in connection with the activities carried out by financial agents and financial advisors, the level of vulnerability was identified at the medium level - a numerical expression 0.57.



A financial agent is a person who performs financial intermediation on the basis of a written contract with a financial institution or on the basis of a written contract with an independent financial agent. At the time of the evaluation, three basic categories of financial agents were distinguished:

- independent financial agent,
- tied financial agent, and
- subordinate financial agent.

In the capital market sector, financial intermediation is provided by the so-called tied investment agent.

At the end of the evaluated period, the following agents operated in the territory of the Slovak Republic:

- 634 independent financial agents,
- 15 618 tied financial agents, and
- 17 847 subordinate financial agents.

A financial advisor is a person who provides financial advice on the basis of a written agreement to provide financial advice to a client. A financial advisor cannot perform financial intermediation.

At the end of the evaluated period, the following advisors operated in the territory of the Slovak Republic SR:

- 12 financial advisors.

Activities of a financial agent and a financial advisor are governed by the general legal regulation⁵⁷, which clearly defines the areas in which they can mediate financial products, or provide financial advice:

- insurance and reinsurance,
- capital market,
- supplementary pension saving,
- receiving deposits,
- extension of loans and consumer credits,
- old-age pension saving.

Supervision of the activities of an independent financial agent and financial advisor is performed by the NBS. Thus, responsibility for the performance of subordinate entities' activities by tied financial agents and subordinate financial agents is taken either by a financial institution or by an independent financial agent over which they perform the so-called transferred supervision. Subsequently, the NBS checks whether the requirements of the Act are fulfilled within the scope of the transferred supervision. The performance of control for AML / CTF measures is primarily within the competence of FSJ, but the NBS has a mandate to perform AML / CTF supervision.

In their business, financial agents are entitled to collect funds under a contract with a financial institution, but only through non-cash payments to a special agent's financial account opened for collection at a bank or branch of a foreign bank.

On the basis of the internal characteristics of the products and services provided, the entities may be misused to commit fraud (including credit and insurance) and the falsification and alteration of a public instrument, official seal, official seal-off, official emblem and official mark, while it should be stressed that the ultimate responsibility for these activities is taken over by the financial institution whose products the financial agent offers, i.e. not the financial agent. In this respect, the financial agent is primarily responsible for the proper identification of the client, and subsequent payments are made by direct cash to the account of financial institutions. The only exception is the collection, where the risk is again minimum for financial agents, because the law foresees that the payment to a special account of an intermediary that is solely for that purpose is a payment for the financial product of the financial institution.

The level of vulnerability is adversely affected by a high number of obliged entities, an activity based solely on the intermediation of products of other institutions.

Determination of priorities in activities of relevant bodies:

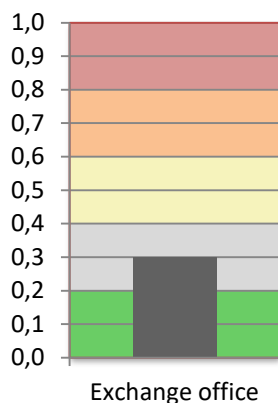
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

⁵⁷ Act No. 186/2009 Coll. on Financial Intermediation and Financial Counselling and on amendments and supplements to certain laws, as amended

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
3.	Effectiveness of UTR reporting and monitoring
4.	Availability and enforcement of criminal sanctions
5.	Effectiveness of compliance function (organization)
6.	Availability and access to BO information
7.	Availability of independent information sources

C. LEGAL ENTITY OR NATURAL PERSON AUTHORIZED TO CARRY OUT EXCHANGE ACTIVITIES – EXCHANGE OFFICE

On the basis of the evaluation of data and information obtained in connection with the activities carried out by legal entities or natural persons authorized to carry out exchange activities – exchange office, the level of vulnerability was identified at the medium-low level - a numerical expression 0.30.



Trading in foreign exchange assets can be performed in the territory of the Slovak Republic only on the basis of a trade license. To obtain it, special conditions must be met – an exchange license must be obtained which is issued by the NBS. The general law⁵⁸ regulates the conditions and activities of exchange offices. At the end of the period under review, a total of 2525 entities were registered, which had a foreign exchange activity in the business. 1604 subjects are listed in the NBS List of Foreign Exchange Points. However,

⁵⁸ Act No. 202/1995 Coll. Foreign Exchange and Act amending and supplementing the Act of the Slovak National Council No. 372/1990 Coll. on Offenses, as amended.

according to this list, it is not possible to identify the exact number of entities currently engaged in this activity. Competent authorities do not have this information available.

NBS staff only perform foreign exchange supervision. Foreign Exchange Act does not entitle them to perform AML / CTF supervision. The performance of control for AML / CTF measures is performed only by FSJ

The level of vulnerability is adversely affected by exclusive use of cash.

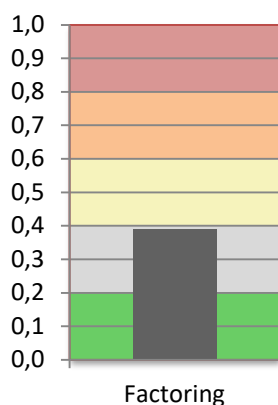
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
2.	Effectiveness of compliance function (organization)
4.	Effectiveness of UTR reporting and monitoring
5.	Availability and enforcement of criminal sanctions
6.	Availability and access to BO information
7.	Availability and enforcement of administrative sanctions
8.	Availability of independent information sources

D. LEGAL PERSON OR A NATURAL PERSON AUTHORIZED TO SELL ACCOUNTS RECEIVABLE - FACTORING

On the basis of the evaluation of data and information obtained in connection with the activities carried out by legal persons or natural persons authorized to sell accounts receivable - factoring, the level of vulnerability was identified at the medium-low level - a numerical expression 0.39.



The authorization to trade in receivables is unqualified notifiable trade, while their activity is generally regulated by Act no. 40/1964 Civil Code, as amended. When issuing a trade license, the entity is not warned that in connection with the performance of this trade he is obliged to fulfil the obligations of the obliged entity established by AML / CTF by Act.

The number of entities with this sphere of business registered has stabilized at 48,358 at the end of the reporting period. However, the exact number of entities active in the business cannot be identified. Many entities have registered this business as a sphere of business but do not actually carry it out. Competent authorities do not have accurate information available.

The inspection of AML / CTF measures is performed exclusively by FSJ.

On the basis of the internal characteristics of the products and services provided, the entities may be misused to commit fraud or tax crime.

The level of vulnerability is adversely affected by the high number of obliged entities and the ability to make cash payments.

Determination of priorities in activities of relevant bodies:

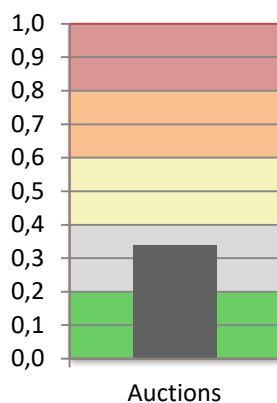
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
3.	Availability and enforceability of input controls
4.	Effectiveness of UTR reporting and monitoring

5.	Availability and enforcement of criminal sanctions
6.	Effectiveness of compliance function (organization)
7.	Availability and access to BO information
8.	Availability and enforcement of administrative sanctions
9.	Availability of independent information sources

E. LEGAL ENTITY OR A NATURAL PERSON AUTHORIZED TO CARRY OUT AUCTIONS OUT OF DISTRAINMENTS – AUCTIONS

On the basis of the evaluation of data and information obtained in connection with the activities carried out by legal entities or a natural persons authorized to carry out auctions out of distraintments, the level of vulnerability was identified at the medium-low level - a numerical expression 0.34.



The general activity of auctioneers is governed by Act no. 527/2002 Coll. Voluntary auction and on amendment of the Act of the Slovak National Council no. 323/1992 Coll. on Notaries and Notarial Activities, as amended. There is no reference to the AML/CTF Act in this law.

The general inspection of compliance with the conditions for organizing and conducting auctions is carried out by the Ministry of Justice of the Slovak Republic. The performance of AML / CTF control measures is performed only by FSJ. The number of entities with the sphere of business at the end of the evaluated period stabilized at 1238, and since 2010 it has been continuously increasing (in 2010, there are 598 entities). However, the exact number of entities active in this activity cannot be identified. Competent authorities do not have accurate information available.

The relevant legislation allows payments to be made in relation to the cash auction. Auctioneers themselves consider this option to be high-risk in terms of money laundering.

The level of vulnerability is adversely affected by the possibility to use cash.

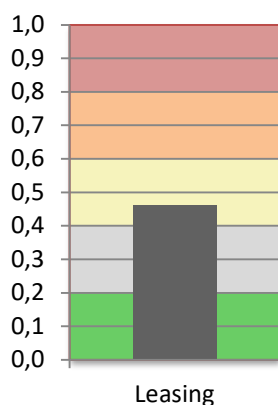
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
3.	Effectiveness of UTR reporting and monitoring
4.	Availability and enforcement of criminal sanctions
5.	Effectiveness of compliance function (organization)
6.	Availability and access to BO information
7.	Availability and enforcement of administrative sanctions
8.	Availability of independent information sources

F. FINANCE LEASE OR OTHER FINANCIAL SERVICES UNDER A SPECIAL REGULATION - LEASING

On the basis of the evaluation of data and information obtained in connection with the activities carried out by entities providing finance lease or other financial services under a special regulation, the level of vulnerability was identified at the medium level - a numerical expression 0.46.



The authorization to provide finance lease or other financial services is unqualified notifiable trade, while this activity is generally regulated by Act no. 40/1964 Civil Code, as amended.

The number of entities with this sphere of business in the end of the period under review stabilized at 41,701 while continuously increasing since 2010 (16,815 entities in 2010). However, the exact number of entities active in this activity cannot be identified. Many entities have registered this business as a sphere of business but do not actually carry it out. Competent authorities do not have accurate information available. They have the option of using the cash in the performance of their activities, but they use it only to a very limited extent. The proportion of international transactions is negligible as a majority of clients are residents.

The inspection of AML / CTF measures is performed only by FSJ.

On the basis of the internal characteristics of the products and services provided, the entities may be misused to commit fraud or tax crime.

The level of vulnerability is adversely affected by the high number of obliged entities and the ability to make cash payments.

Determination of priorities in activities of relevant bodies:

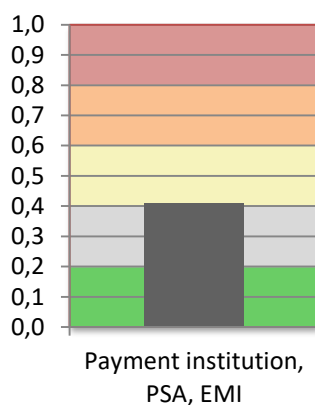
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities

3.	Availability and enforceability of input controls
4.	Availability and enforcement of criminal sanctions
5.	Effectiveness of compliance function (organization)
6.	Availability and access to BO information
7.	Effectiveness of UTR reporting and monitoring
8.	Availability and enforcement of administrative sanctions
9.	Availability of independent information sources

G. PAYMENT INSTITUTION, A PAYMENT SERVICE AGENT AND AN ELECTRONIC MONEY INSTITUTION

On the basis of the evaluation of data and information obtained in connection with the activities carried out by payment institutions, payment service agents and an electronic money institutions, the level of vulnerability was identified at the medium level - a numerical expression 0.41.



A payment institution is a person providing payment services without limitation or to a limited extent. NBS approval is required. It may also provide payment services through a payment service agent. At the end of the period under review, the number of payment institutions stabilized at 9, and since 2010 it has been continuously increasing (in 2010, we had 1 payment institution). The total number of registered foreign payment institutions is 218. At the end of the reporting period, the number of agents of payment institutions was at 2.

An electronic money institution is a person who is authorized to issue electronic money, manage electronic money, and execute payment operations. NBS approval is required. At

the end of the period under review, there was 1 electronic money institution in the SR. The total number of registered foreign electronic money institutions is 96.

The general activities of these entities are governed by Act no. 492/2009 Coll. on Payment Services and on Amendments and Supplements to Certain Acts, as amended. The control of AML / CTF measures is primarily within the competence of FSJ, but the NBS has a mandate to perform AML / CTF supervision.

In their activity, they are allowed to use cash under the law. The share of international transactions is high, the value of funds sent to the Slovak Republic is very high. Given the internal characteristics of the products and services provided, it is possible for transfers of funds to be executed in certain cases without the client's physical presence.

Based on the internal characteristics of the products and services provided, the entities may be misused to commit fraud (especially phishing).

The vulnerability level is affected by the ability to make cash payments and use products without the client's physical presence.

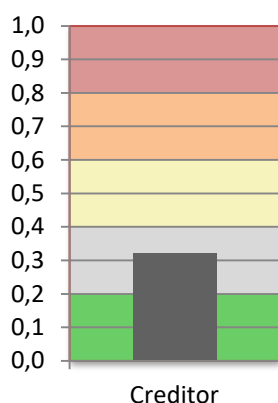
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities
3.	Availability and enforcement of criminal sanctions
4.	Availability and access to BO information
5.	Effectiveness of UTR reporting and monitoring
6.	Availability of independent information sources

H. CREDITOR

On the basis of the evaluation of data and information obtained in connection with the activities carried out by creditors, the level of vulnerability was identified at the medium-low level - a numerical expression 0.32.



A creditor is a person offering or providing consumer credits. General activity and position of creditors is regulated by Act no. 129/2010 Coll. consumer credits and other credits and loans for consumers and on amendments and supplements to certain laws, as amended. NBS approval is required. At the end of the period under review, the NBS registered a total of 26 creditors.

In their activity, they are allowed to use cash under the law, but they use it only to a very limited extent. The proportion of international transactions is negligible as a majority of clients are residents. The law also makes it possible to use separate financial agents and tied financial agents for consumer credits. At present, creditors use 2,775 tied financial agents .

On the basis of the internal characteristics of the products and services provided, the entities may be misused to commit the fraud and criminal offense of falsification and alteration of a public instrument, official seal, official seal-off, official emblem and official mark, while it , official seal, official seal, official emblem and official mark.

The vulnerability level is adversely affected by the ability to make cash payments, using products without the physical presence of the client, and providing products through a high number of intermediaries.

Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the OFI sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
2.	Effectiveness of supervision and control activities

3.	Availability and enforcement of criminal sanctions
4.	Availability and access to BO information
5.	Effectiveness of UTR reporting and monitoring
6.	Availability of independent information sources

2.4. INSURANCE SECTOR

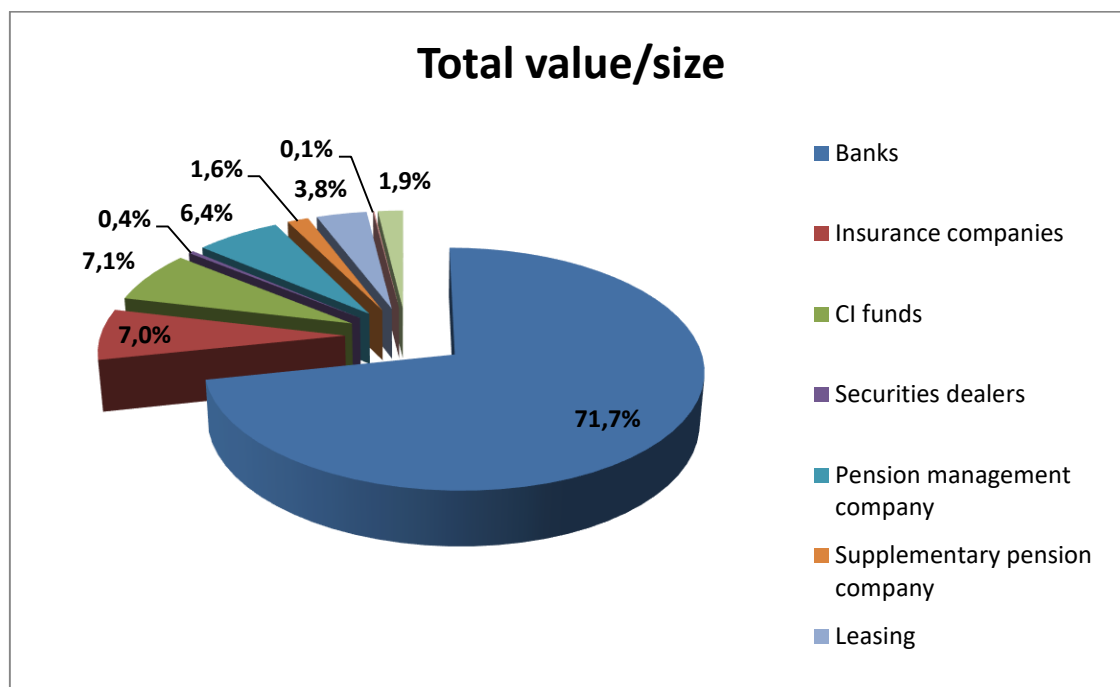
GENERAL INFORMATION ON THE INSURANCE SECTOR IN THE SLOVAK REPUBLIC

The insurance sector has an irreplaceable function in the process of economic, social and legal functioning of every society. The standard of living, prosperity and economic growth of the society can also be increased by limiting risks from unexpected and accidental events. The role of insurance is to compensate or mitigate damage to property or health.

In the period under review, the following entities operated in the Slovak insurance market:

- 16 insurance companies based in the SR,
- 20 insurance companies based in another EU State through a branch, and
- 605 insurance companies based in another EU State without a branch, on the basis of free provision of services.

The total share of insurance companies' assets in financial market entities was approximately 7 %.



The value of the product in the insurance sector is mainly determined by technical premiums. At the end of the period under review, the total amount of technical premium was 2 019 804 ths. EUR, whereas:

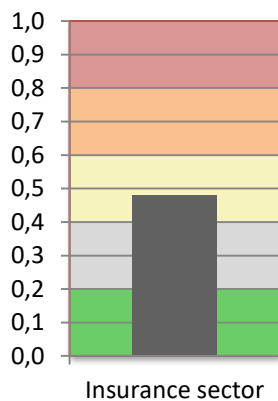
- the share of life insurance was 52.2%, which represents assets of 1,054,488 ths. EUR,
 - o Out of it, investment life insurance of 300,024 ths. EUR,
- the share of non-life insurance was 47.8 %, which represents assets of 965,316 ths. EUR.

At the end of the period under review, insurance companies had technical provisions in the total amount of 4,715,173 ths. EUR, whereas:

- in life insurance, insurers generated technical provisions of 3,792,968 ths. EUR, which is 80.4%,
 - o Out of it, provisions for the coverage of liabilities from realisation on investments on behalf of insured persons (investment life insurance) in the amount of 1,144,046 ths. EUR,
- in non-life insurance, insurers generated technical provisions of 922.205 ths. EUR, which is a 19.6% share.

VULNERABILITY OF THE INSURANCE SECTOR

In the SR, on the basis of the evaluation of data and information obtained, the level of vulnerability of the insurance sector was identified at the medium level - a numerical expression 0.48 – see the graph.



In the analysis of the insurance sector, the following facts were taken into account:

- Segment size,
- Nature of insurance products,
- Nature of prospective clients,
- Sales channels,
- Insurance sector regulation.

PROCEDURAL VULNERABILITY

VULNERABILITIES IN INSURANCE SECTOR

In the insurance sector, based on input data, **the risk score was set at 0.48 - medium at the bottom**. This means that the risk of money laundering in this area is present, but to a limited extent, taking into account the size of the insurance sector within the financial

market, the nature of insurance products, the nature of prospective clients, sales channels as well as sufficient regulation of the insurance sector.

The assessment of the insurance sector in terms of AML focused on life insurance and non-life insurance. In life insurance, the subject of assessment was investment life insurance (the so-called unit-linked) separately as an insurance segment life, for which increased ML risk was identified, and traditional life insurance (insurance against death, endowment insurance, pension insurance). A higher ML risk for unit-linked products results mainly from the possibilities of investment for the clients in the form of one-off deposits or repeated deposits and withdrawals. The products are primarily linked to an investment component of the contract, and not to traditional insurance risk (death, reaching a certain age). For unit-linked insurance, the procedure of taking out contracts including the client identification as well as the verification of the origin of funds is identical to the procedure used by insurers to take out other life insurance contracts, i.e. the approach to these clients is the same despite a higher risk of legalization. The highest ML / TF risk in the sector is for clients with unclear ownership structure and when a legal entity as a prospective client cannot sufficiently demonstrate from what sources it has received the funds it possesses.

In general, no specific ML / TF risks are perceived in the insurance sector as long as clients funds are received or sent to the institution solely through non-cash bank transfers and such transfers are covered by standard arrangements for the transfer of funds (Article 10, Article 12, Article 14 AML/CTF Act).

Transactions executed on behalf of another person, non-transparent follow-up transactions, transfers of funds between entities domiciled in different countries, receiving funds from clients from non-standard countries and regions, such as off-shore zones, risky, sanctioned countries, etc., and also situations where it is assumed that such clients have high volumes of funds the origin of which may be unclear in terms of AML, may pose a risk.

The following vulnerabilities have been identified by assessing the procedural aspects related to the activities and internal processes of individual businesses in the insurance sector as well as to the supervisory / control authorities:

- a. Low number of controls / supervision by competent authorities,
- b. Insufficient enforcement of administrative sanctions,
- c. Insufficient application of AML/CTF legislation by insurance sector businesses,
- d. Ineffective application of AML/CTF preventive measures,
- e. Insufficient knowledge of insurance companies staff about ML/TF risks and their management,
- f. Effectiveness of UTR monitoring and reporting,
- g. Non-acceptance of insurers requests for data and source materials under Article 13 par. 1 of AML/CTF Act by banks, mainly the verification of data of the holders of relevant contact bank accounts stated in contracts.

Detailed analysis of selected vulnerabilities in the insurance sector

- a) Low number of controls / supervision checks by competent bodies,

During the period under review, the subject of NBS's AML / CTF supervision was a relatively low number of businesses operating in the insurance sector. Likewise, FSJ carried out a low number of compliance checks for with AML/CTF obligations. The reason for the vulnerability in the field of inspection is the fact that FSJ does not have sufficient resources (financial and technical), and trained staff to ensure efficient and adequate inspection. The understaffed FSJ caused that in the period under review, FSJ executed only a very low number of inspections in the insurance sector. With respect to a lack of funds and workload, the FSJ members did not have a chance to acquire necessary skills and up-to-date knowledge for inspection of AML/CTF compliance through paid professional seminars, training and conferences.

b) Insufficient enforcement of administrative sanctions

In the period under review, the sanctions in the form of fines were imposed by FSJ were only in the lower bands with respect to their preventive action and educational character. The low number of fines and their amount did not have sufficient preventive and dissuasive effect. As follows from the results of the supervision of insurance companies as obliged entities, they continue to fail to comply with all obligations arising from the AML/CTF Act.

The NBS's approach with respect to sanctions, which did not impose any sanctions (fines or remedies) for the breach of AML/CTF obligations may be considered a vulnerability in the period under review, can also be considered a vulnerable area.

c) Insufficient application of AML/CTF legislation by insurance sector businesses

In particular, the following shortcomings were identified during NBS and FSJ inspections / controls performed with the businesses:

- Absence of obligatory elements in own activity programme, (e.g., own activity programme did not contain specific ML/TF risks, as well as their division for the purpose of identification of risk and subsequent performance of adequate CDD measures),
- Absence of a risk-oriented approach and the non-inclusion of clients in risky groups,
- Failure to identify the origin of funds,
- Failure to take appropriate measures to identify the ownership and management structure of clients,
- Failure to take appropriate measures to verify the identification of beneficial owner,
- Failure to report UTRs without undue delay,
- Failure to assess individual transactions and to keep records of transaction assessments,
- Failure to perform the relevant type and scope of CDD,
- Incompleteness of insurance policies in terms of AML / CTF measures:
 - o Absence of a binding written statement by the client about the ownership of the funds and a statement that he acts on his own behalf,
 - o Insurance companies did not prove that in the case of some insurance contracts they had identified whether the client was acting on his own behalf,

- Insufficient application of legal obligations during client identification (Article 7 par. 1 a)⁵⁹ or b)⁶⁰ AML/CTF Act)

An important inspection finding was the identification of the insurance product provided by the insurer with a high level of ML / TF vulnerability - the so-called special insurance account. In this case, the insurance is taken out only against client's death. A part of the product is the possibility to perform an above-standard assessment of the client's funds, which are not related to insurance and allow very high one-time deposits of the client. The Insurance account allows clients to make deposits, withdrawals and transfers of funds from any payment accounts held in banks and branches of foreign banks in the Slovak Republic. Given the internal characteristics of this product, this product was identified by FSJ as high risk.

d) Ineffective application of AML/CTF preventive measures

Vulnerability in this area is mainly due to the fact that insurance products are easily available, and insurers are primarily dependent on financial intermediaries. During the period under review, some obliged entities in the insurance sector did not pay sufficient attention to the preventive measures resulting from the AML/CTF Act and exposed themselves and the legal financial system to risk of possible legalization.

Vulnerability resulting from the ineffective application of preventive measures was identified in particular in relation to:

- Insufficient consideration of the risks arising from AML and CTF in the assessment and management of their risks,
- Failure to perform controls for the performance of AML/CTF obligations (internal or external audits), or with a significant time gap,
- Absence of a list of tax havens (off-shore countries),
- Non-inclusion of a responsible person for AML as a senior employee,
- Insufficient knowledge of insurance companies staff about ML/TF risks and their management,

e) Insufficient knowledge of insurance companies staff about ML/TF risks and their management

Shortcomings in employee training and employee knowledge verification are a significant vulnerability. Vulnerability is mainly related to the irregularity of employee testing, but mainly to the inconsistent performance of training in the theoretical field and practical aspects of assessing clients and their transactions, CDD performance and UTR reporting. For

⁵⁹ Article 7 par. 1 a), in the case of a natural person, the identification of the name, surname, birth number or date of birth, permanent address or other residence, nationality, type and number of identity document; for a natural person-entrepreneur, the address of the place of business, the identification number, if any, the identification of the official register or other official register in which the entrepreneur is registered, and the registration number in that register or record,

⁶⁰ Article 7 par. 1 b) in the case of a legal entity, the identification of the name, address of the registered office, identification number, identification of the official register or other official register in which the legal person is registered and the registration number in that register or record, and the identification of the natural person authorized to act on behalf of the legal entity.

some entities, there were no special training courses for selected employees or financial intermediaries who may be exposed to more frequent (and more sophisticated) attempts to misuse the insurance sector's products for ML and TF. Not all insurers warn employees within internal training of the criminal-law consequences of violating legal AML/CTF obligations.

Insufficient knowledge of ML/TF risks was reflected in the detailed assessment of individual reports, as a significant part of the reported operations were to be assessed by the insurance companies as usual. Obviously, in most cases, insurance companies reported all operations that had one of the form of UTRs listed in their own activity program without carrying out the appropriate type and scope of customer due diligence.

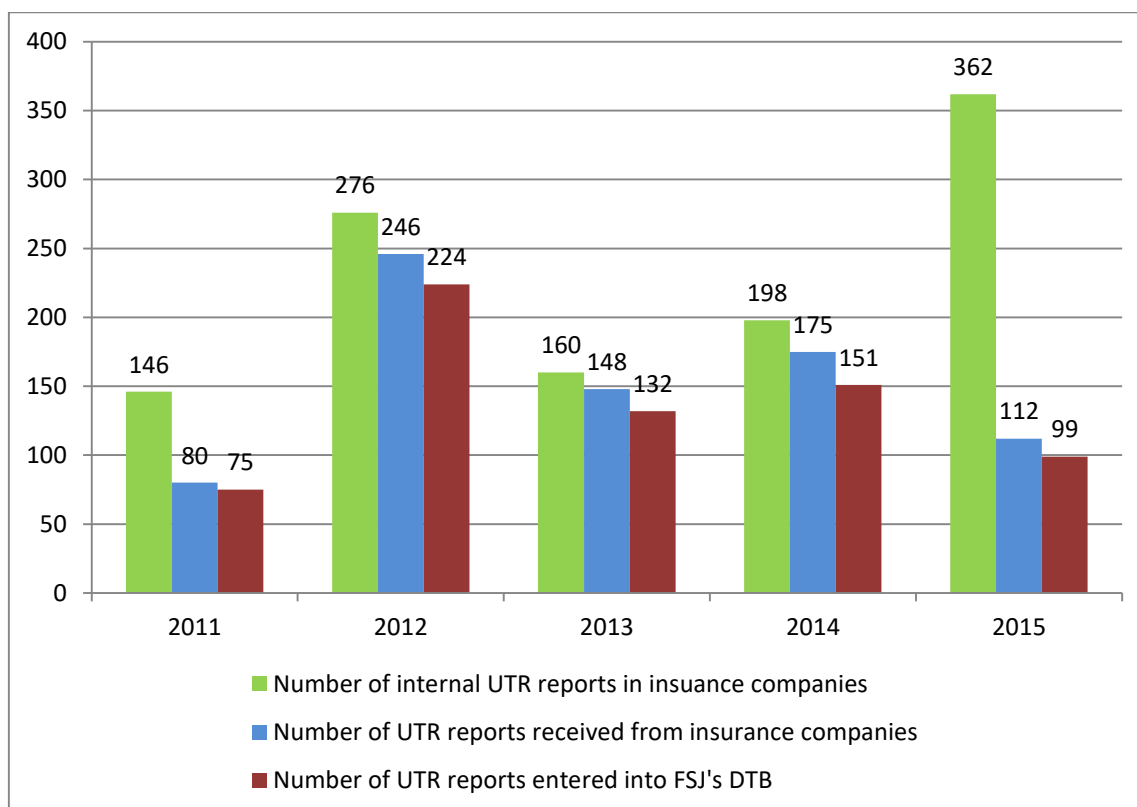
f) Effectiveness of UTR monitoring and reporting

The adverse impact and thus the increased vulnerability of products in the insurance sector are clients with unclear ownership structure and cases where the client is unable to demonstrate in a sufficient and reliable manner the origin and source of the funds at his disposal. Especially if he has a high volume of funds. Transactions and business relations are also vulnerable from the point of view of unclear follow-up transactions, transfers of funds between entities based in different countries, receipt of funds from clients based or residing in high-risk countries, tax havens (off-shore countries), or sanctioned countries.

In particular, "post-transaction" manual monitoring has a negative impact on the vulnerability related to transaction monitoring and the client. Most insurance companies do not use automated monitoring systems, nor do they use an automated monitoring system to check sanction lists and PEPs. Several insurance companies declared that they were working on the development of automated systems.

In the period under review, FSJ received and verified a total of 761 UTR reports. Based on a detailed analysis, the following vulnerabilities in UTR monitoring and reporting were identified:

- Inconsistent CDD,
- When assessing transactions, no emphasis is placed on identifying the origin of funds entering the system,
- UTR reporting focuses on the exit of funds (redemption, termination of insurance) from the insurance segment),
- For UTR reports, absence of information on CDD performed,
- Transactions or the client being the subject of UTR is not subsequently moved into a higher risk category,
- When processing UTR reports by subsequent verification of facts, it was found out that compliance personnel only had formal knowledge of AML/CTF.
- For most of the UTR reports it was not clear for what reason the transaction was assessed as unusual,
- For most of the UTR reports it was not clear what type (and what scope) of CDD was performed by the insurer,
- Overall poor quality of UTR assessment and reporting, as well as transaction assessment records.



Dynamics of the development of the number of UTR reports in insurance and the effectiveness of their use

g) Non-acceptance of insurers requests for data and source materials under Article 13 par. 1 of AML/CTF Act by banks, mainly the verification of data of the holders of relevant contact bank accounts stated in contracts

Funds related to insurance contracts (premiums, payment of insurance benefits) are usually transferred through cash payments, whether in banks or branches of foreign banks, or through the offices of Slovenska posta, a.s. In this respect, it should be stressed that banks (and branches of foreign banks), including the postal company, are obliged entities, due to which they are obliged to comply with the measures specified in the AML / CTF Act. As in the case of the securities sector, in the case of the insurance sector, banks and branches of foreign banks represent an important "buffer zone" on the entry of potentially illegal funds into the legal financial system.

Vulnerability, in addition to the insufficient acceptance of CDD measures by banks and branches of foreign banks, is the refusal to provide or verify information about clients of insurance companies, which the particular insurance company discovered during the performance of CDD – the so-called performance by third parties⁶¹. During the period under review, banks and branches of foreign banks did not accept the requests for data and source materials submitted by insurance companies.

⁶¹ Reference to Article 13 par. 1 AML/CTF Act effective in the period under review

ANALYSIS OF INSURANCE SECTOR BUSINESSES

GENERAL ANALYSIS

Insurance companies use both internal network and external to sell their products, where insurance products are offered through financial intermediaries, through independent financial agents (IFAs), subordinate financial agents (SFAs) or tied financial agents (TFAs). More than 70% of the insurance sector's production is offered through financial intermediaries.

Insurance companies are the entities which, on the basis of all the information available (i.e. not only obtained from contract management), determine the factors necessary for the categorization of clients and their transactions, and also determine the characteristics needed to identify the potential for legalization and unusual transactions, as well as the appropriate level to reduce identified risks (type and extent of CDD, including assessment of transactions and performance of measures under AML Act). It should be noted that the **ultimate responsibility for carrying out complete CDD in relation to the client is borne by the insurance company (objective liability)**, despite the fact that financial intermediaries are also classified as obliged entities within the meaning of Article 5 of the AML Act.

In most cases, the premium is paid to the bank account or by postal order. Insurance companies pay out insurance benefits solely to the bank account or by postal order to the address of the beneficiary. Insurance companies based in the Slovak Republic provide insurance products across the EU only to a limited extent, mainly non-life products (e.g. property insurance, travel insurance, liability insurance, etc.). The Slovak law does not allow anonymous provision of products. This means that the internal rules and procedures of insurance companies in accordance with AML/CTF provide for the obligation to refuse to enter into a business relationship if the client refuses to identify himself when concluding an insurance contract or refuses to declare on whose behalf he acts. Insurance companies proceed equally in case of insufficient identification of the person entitled to the insurance benefit, i.e. the beneficiary from the insurance contract must always be known. It is possible to conclude insurance contracts for a certain type of products impersonally. These are mainly non-life insurance products (e.g., travel insurance, accident insurance, compulsory liability insurance, property insurance, etc.). Impersonal form of insurance means online insurance via Internet, SMS insurance, call centre (insurance taken out through the telephone services department), direct mail and insurance products concluded through selected financial intermediaries.

In the period under review, there was no recorded case of money laundering in the Slovak Republic. There have been cases where insurance products were used for fraudulent activities, in particular non-life insurance (accident insurance, compulsory liability insurance, property insurance, etc.). In most cases, it is mainly fraudulent insured events in motor insurance. As for the reputation of insurance companies for participation in financial crimes, including tax evasion, it can be assessed that no insurance company was reported in Slovakia to have been associated with participation in financial crimes, including tax evasion.

In the period under review, insurance companies did not report any suspicion of committing an intentional criminal property-related offense by employees. Insurance companies also do not report any employees who violate internal rules to avoid conflicts of interest, insider trading, or abuse of confidential information. In connection with the breach of AML/CTF obligations, no motion was filed by insurance sector businesses to initiate criminal proceedings against an employee.

a) Legal regulation of the insurance sector

The legal system of the Slovak Republic has comprehensive laws concerning AML and CTF preventive measures, as well as the control and supervision of entities carrying on business activities in the insurance sector. In addition to the Slovak legally binding regulations, EU legal acts, international standards and, last but not least, knowledge, practical experience and generalized results of FSJ inspections or NBS supervision, also contribute to the regulation of business activities in the insurance sector.

The legal regulation of individual concepts and the obligations implemented in the field of AML and CTF is primarily contained in the AML/CTF Act. This Act regulates the obligation to apply a risk-oriented approach to clients. Obligated entities in the securities sector must have an overview of the potential risks associated with a particular client. On the basis of the information obtained, they are obliged to determine the extent of CDD and, if necessary, to apply enhanced due diligence.

General legislation⁶² regulates the rights and obligations of insurance sector businesses, while in the case of persons managing an insurance company or performing key functions, the law assumes that the requirements for professional competence and credibility are met. The condition of the credibility of employees of insurance companies is regulated by internal rules of the insurance companies, whereas most insurers require, for the purpose of proving the credibility of employees, not only a statement of criminal records, but also an affidavit of several facts demonstrating their credibility or, if appropriate, other documents including a performance assessment from the previous employer.

The legislation on the imposition of criminal sanctions is complex and sufficient. However, in practice, such sanctions have not been imposed at all. It should also be noted that the deterrent effect of criminal sanctions is being weakened due to the application of the so-called "active repentance" in accordance with the relevant provisions of the Criminal Act. This means that the punishability of an offense ceases to exist, if the offender has voluntarily prevented or remedied the harmful effect of the offense.

The complexity of the above legislation for the activities of insurance sector businesses is also complemented by detailed explanations on the fulfilment of obligations arising from legal regulations prepared in the form of an NBS Methodological Guideline⁶³ and FSJ Methodological Guidelines⁶⁴.

⁶² Act No. 39/2015 Coll. on Insurance and on amending and supplementing certain laws, as amended

⁶³ Methodological Guideline of the Financial Market Supervision Unit of the NBS of 4 October 2013 no. 4/2013 for the protection of an insurance company, a branch of an insurance company from another EU Member State

The legal regulations lack subordinate legislation (e.g. in the form of a decree or measure) specifying the individual areas and content of obligations for insurance companies, which are generally regulated by the AML/CTF Act. Currently effective NBS Methodological Guidance has only a recommendatory and non-binding character.

b) Internal AML/CTF regulations

The Code of Conduct for employees of insurance sector businesses is regulated by internal regulations, which are regularly updated and available to all employees through the internal network (Intranet). As a rule, they are aimed at preventing conflicts of interest, insider trading, or abuse of confidential information. Internal regulations also have mechanisms in place to protect employees from the negative consequences and risks resulting from UTR reporting.

Board of Directors, under whose direct control is the position of the so-called designated person, has the responsibility for the overall AML/CTF protection of insurers. In specific cases, the designated person is under direct control of the Managing Director. The designated person is responsible for the practical implementation of AML/CTF measures. The independence of the function is determined by its separation from operative and commercial activities, including the unlimited right to communicate with employees and access to information relevant to the exercise of his rights and obligations.

In most insurance companies, the position of the responsible person for AML is part of the key compliance function. Other insurance companies have a responsible person for AML in the organizational structure included in the position of senior employee. In several insurance companies, the responsible person for AML is not included in the position of senior employee. At the same time, it can be stated that most of insurance companies are adequately staffed.

The basic internal regulation for AML methodological provision in insurance companies is an AML Programme, which is intended for all employees. The overall level of knowledge and awareness of AML/CTF responsibilities among the staff is high. This level also takes into account some weaknesses, especially in the area of client categorization, identification of the BO, monitoring of PEPs and sanctioned persons.

Determination of priorities in activities of relevant bodies:

and a branch of an insurance company from a non-EU Member State against money laundering and terrorist financing

⁶⁴ FSJ's website, <http://www.minv.sk/?Metodicke-usmernenia-a-stanoviska-FSJ>

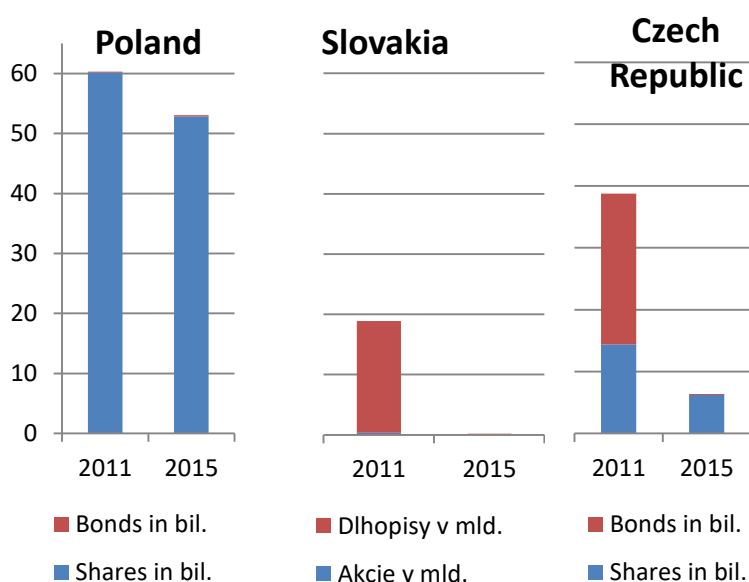
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the insurance sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of procedures and practical aspects of supervision
2.	Availability and enforcement of sanctions (administrative and criminal)
3.	Consistent application of AML/CTF legislation by entities
4.	Effective implementation of preventive AML/CTF measures by businesses
5.	AML/CTF awareness of insurers staff
6.	Effectiveness of UTR monitoring and reporting
7.	Availability and access to BO information

2.5. SECURITIES SECTOR

GENERAL INFORMATION ON THE SECURITIES SECTOR IN THE SLOVAK REPUBLIC

The capital market has developed in SR's conditions as a by-product of Voucher privatization, whereas it focuses mainly on trading in bonds. Trading in stocks has a minimum level. Despite these particularities, a decline of investors' interest in trading on the Slovak capital market is evident, as evidenced by the long-term decrease in traded volumes over the period under review.



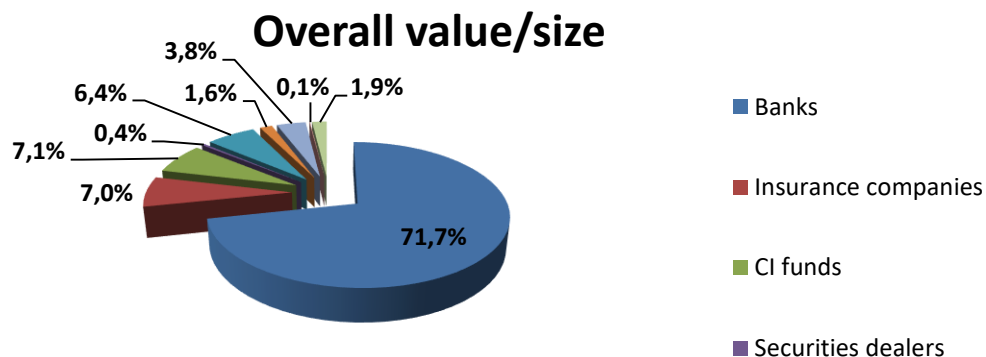
With regard to the evaluation of basic capital market parameters (type of capital, assets under management, share and bond issues), the Slovak capital market is among the least functional among EU countries. This fact is negatively affected in particular by the minimum stock market liquidity, high cost and administrative burden on prospective participants. Investors do not regard the Slovak stock market as an investment opportunity due to the absence of high-quality domestic shares, high fees and a low-diversified market.

In the period under review, the following entities operated in the securities sector. These entities are also considered obliged entities in terms of AML/CTF obligations.

- Central Securities Depository, operates on the basis of a license from the NBS and its 100% shareholder is BCPB, performs activities based on membership and had 20 members in the period under review.

- Stock exchange: During the period under review, it had 14 shareholders, the largest shareholder being the National Property Fund of the Slovak Republic,
- Asset management company: During the period under review, six domestic asset management companies and one foreign asset management company operating 87 domestic open-ended mutual funds were active,
- Securities dealer: During the period under review, 14 non-bank securities dealers; 17 banks and branches of foreign banks and 2 asset management companies were active,
- Pension management company: During the period under review, 6 pension management companies that managed a total of 20 pension funds, and
- Supplementary pension company: During the period under review, there were 4 supplementary pension companies that managed a total of 17 supplementary pension funds.

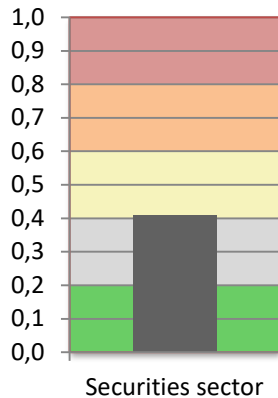
The overall market capitalization of shares (financial market instruments) in GDP in the Slovak Republic ranged between 4% and 6% of GDP.



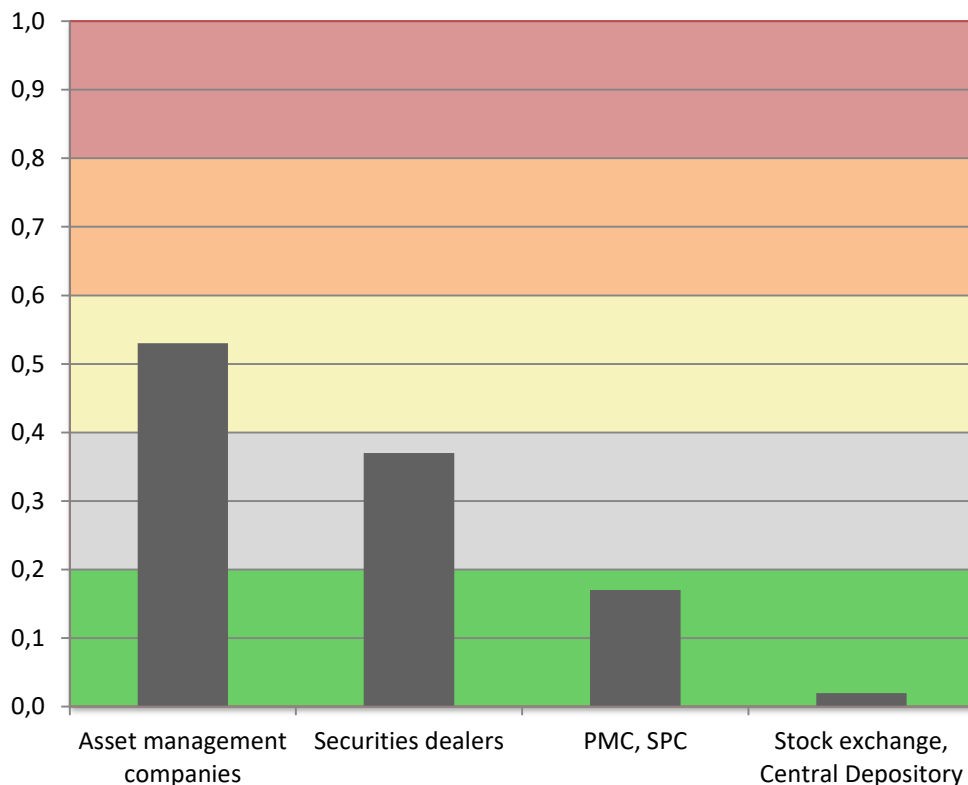
Share of individual financial sectors in financial sector assets

VULNERABILITIES OF THE SECURITIES SECTOR

In the SR, on the basis of the evaluation of data and information obtained, the level of vulnerability of the securities sector was identified at the medium level - a numerical expression 0.41 – see the graph.



Comparative graph of the vulnerability levels of individual entities of the securities sector



In analysing the securities sector, the following facts were taken into account:

- Segment size,
- Estimated volume of assets managed by clients,
- Number of reported UTRs,

- Level of exposure to ML/TF threats,
- Importance for detecting threats,
- Severity and diversity of threats, and so on.

PROCEDURAL VULNERABILITY

VULNERABILITIES IN THE SECURITIES SECTOR

The following vulnerabilities were identified by evaluating the procedural aspects related to the performance of the activities and internal processes of the individual securities sector businesses as well as the supervisory and control authorities:

- Insufficient application of legislation,
- Ineffective application of preventive AML/CTF measures,
- Insufficient knowledge and awareness of ML/TF risks and their management,
- Non-standard transactions with financial instruments and transaction monitoring,
- Low number of controls by FSJ,
- Non-imposition of sufficiently deterrent sanctions,
- Low level of cooperation between regulators and professional organizations and obliged entities,
- Absence of central register of BOs,
- Absence of central bank account register.

Detailed analysis of selected vulnerabilities in the securities sector

a) Effectiveness of supervisory procedures and methods (low number of controls by FSJ)

- The long-term vulnerability of FSJ's activities is a lack of personnel, technical and financial resources to enable FSJ members to perform their tasks and responsibilities effectively. The absence of these resources has resulted in the absence of trained staff of the FSJ's Obligated Entities Control Department. Understaffing has an adverse impact on the performance of the necessary controls. The current status does not allow FSJ officers to continuously acquire the necessary skills and up-to-date knowledge required to perform AML/CTF compliance controls due to their workload and lack of financial resources that would cover the necessary costs associated with attending seminars, training or conferences. In this respect, there is an absence of guidelines and recommendations issued, as well as overall educational activity.

b) Insufficient knowledge and awareness of ML/TF risks and their management (knowledge of the securities sector staff about AML measures)

- A low level of awareness of the obliged entities of obligations resulting from the AML/CTF Act also has an adverse effect on the vulnerability level, which is directly linked to understaffing for controls of securities sector businesses. In this context, it is necessary to increase the frequency and quality of internal training, the theoretical training of employees,

especially those who monitor and evaluate client business operations. The changes should also affect the quality of technical support for transaction assessment.

c) Effectiveness of transaction monitoring

-

In the period under review, FSJ received and verified a total of 221 UTR reports. Based on a detailed analysis, the following vulnerabilities in UTR monitoring and reporting were identified:

- Inconsistent implementation of CDD measures and assessment of unusualness,
- When assessing transactions, no emphasis is placed on identifying the origin of funds,
- UTR reporting is oriented to the exit of funds from the financial system (redemption, termination of business relationship),
- No information on the CDD measures in UTRs,
- Risk category of the client does not increase despite the fact that the client is subject to a UTR report,
- Formal shortcomings of designated persons for AML/CTF obligations, resulting in serious shortcomings in the practical application on specific cases,
- Low quality of UTR reporting as well as of transaction assessment records.

d) Insufficient application of legislation

- Consistent compliance with AML/CTF Act and other generally binding legal regulations governing the status, roles and activities of securities sector businesses is a prerequisite for effective prevention.

In the period under review, the NBS carried out a total of 114 supervisory controls in the securities sector:

- a) In the area of collective investment, a breach of legislation was identified with respect to the insufficiently prepared AML/CTF internal regulation; an obliged entity's employment contract did not specify the designated person's responsibility for AM /CTF,
- b) No breaches of AML/CTF Act were identified in the area of pension savings,
- c) In the area of securities, a breach of AML/CTF legislation identified in relation to the non-appointment of a designated person responsible for the AML/CTF; non-compliance with employee training schedule; failure to inform and review the AML Reports by the Board of Directors and the Supervisory Board of the company; insufficiently developed and updated internal regulations; non-evaluation and non-reporting of UTRs.

In the period under review, FSJ performed a total of 3 controls in the securities sector:

- a) In the area of securities market,
- b) In the area of collective investment.

In this context, a breach of legislation was found in connection with the absence of obligatory elements in the obliged entity's own activity program; failure to identify the origin of the funds and to take appropriate measures to identify the ownership and management structure of the client and the subsequent refusal to establish a business relationship; failure to report UTRs without undue delay despite the suspicion of tax crime; improper manual adjustment of AML/CTF client risk, failure to assess individual transactions, failure to keep assessment records, failure to perform enhanced due diligence.

e) No imposition of sufficiently deterrent sanctions

- In the period under review, sanctions (fines) for violating the provisions of the relevant legislation were imposed by FSJ rather in the lower bands with respect to their preventive action and educational character. However, given the shortcomings identified, it can be stated that these sanctions were not sufficiently effective and deterrent.

- The imposition of sanctions is a vulnerability on the part of the NBS. In all supervised entities, the NBS may impose various types of sanctions, including the possibility of a fine on a member of the Board of Directors, a member of the Supervisory Board, and a branch manager in the event of a breach of an obligation under the applicable legal regulations. However, no sanctions (fines or remedies) were imposed in the application practice).

VULNERABILITY OF BANKS AND FOREIGN BANK BRANCHES

A special fact in relation to the assessment of vulnerabilities in the securities sector was the assessment of banks and branches of foreign banks operating in Slovakia.

It is the banking system that plays a key role in placing funds in the securities sector. In this context, a significant vulnerability was identified in monitoring and identifying UTRs in relation to transactions performed to the credit of securities businesses. Bank and foreign bank employees, including financial institution employees coming into contact with clients on the securities market should be trained in UTR recognition. Shortcomings in the banking sector have a subsequent adverse impact on the capital market and, last but not least, on the reputation of the entire financial sector.

ANALYSIS OF SECURITIES SECTOR BUSINESSES

GENERAL ANALYSIS

a) Legal regulation of the securities sector

The legal system of the Slovak Republic has comprehensive generally binding legal regulations concerning AML/CTF preventive measures, as well as the control and supervision of insurance sector businesses. In general, the legal regulations are based not only on Slovak legally binding regulations, but also on international standards and knowledge, practical experience gained in the performance of FSJ control/NBS's supervision.

The legal regulation of individual concepts and the obligations implemented in the field of AML and CTF is primarily contained in the AML/CTF Act. This Act regulates the obligation to apply a risk-oriented approach to clients. Obligated entities in the securities sector must have an overview of the potential risks associated with a particular client. On the basis of the information obtained, they are obliged to determine the extent of CDD and, if necessary, to apply enhanced due diligence.

General legislation regulates the rights and obligations of securities sector businesses. Each of the relevant acts contains provisions regulating employee integrity and credibility. In addition to the obligation to present relevant documents, integrity is verified by a personal interview, references from previous employers and also based on information from public sources. In principle, it is an integral part of the selection process in each of the securities sector businesses. In the case of positions as members of the Board of Directors, proctors and managers under the direct management of the Board of Directors, top management, it is necessary to demonstrate professional competence and credibility.

The complexity of the above legislation for the activities of securities sector is also complemented by detailed explanations on the fulfilment of obligations arising from legal regulations prepared in the form of an NBS Methodological Guidelines and FSJ Methodological Guidance.

b) Internal AML/CTF policies

Obligated entities carrying out their activities within the securities sector are subject to internal rules prohibiting the application of any negative measures to employees responsible for AML/CTF. Institutions shall ensure that these persons perform their activities impartially and independently. They are usually incorporated under the Board of Directors with well-defined rights and obligations and have adequate organizational and material conditions to perform their functions.

The relevant internal rules also regulate the protection of employees against retaliatory measures, who, in good faith, reported suspicion of non-compliance, fraud or corruption.

The overall level of knowledge and awareness of staff of AML/CTF responsibilities is high⁶⁵. This level also takes into account certain shortcomings, particularly in the area of client categorization, detection of BOs, monitoring of PEPs and sanctioned persons or the assessment of transactions.

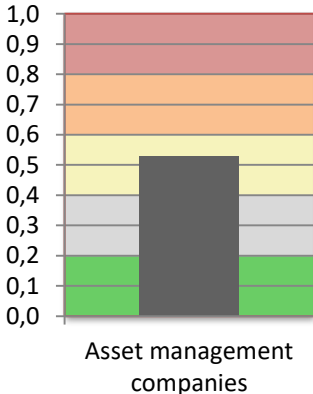
During the period under review, no suspicion of committing an intentional crime of a property nature by employees was recorded. Likewise, no employees are reported who would violate internal rules to prevent conflicts of interest, insider trading, abuse of confidential information, or the cases that employees caused the leakage of protected client information. None of the securities sector businesses have initiated criminal proceedings against employees for violating AML/CTF obligations.

In terms of the reputation of the securities sector during the period under review, it was not reported that these entities were involved in any Criminal offenses of economic nature or Criminal offenses against property, including tax crime.

ML RISK IN INDIVIDUAL SECURITIES SECTOR BUSINESSES

A. ASSET MANAGEMENT COMPANIES (COLLECTIVE INVESTMENT AREA)

On the basis of the evaluation of data and information obtained in connection with the activities carried out in collective investment, the ML risk was identified at the medium level – 0.53.



In particular, the fact that collective investment products are performed in a non-cash way through banking sector businesses or cash operations through financial institutions offices, had a positive effect on the risk level. The amount of cash invested in mutual funds

⁶⁵ This conclusion resulted from the information provided by the relevant institutions. They assessed the average level of knowledge and awareness of their employees as "2" (on a scale of 1 - best to 5 – worst).

is, according to available information, minimum. The fact that "intermediary" businesses of the banking sector are considered as obliged entities under the AML/CTF Act, which obliges them to implement appropriate CDD measures, appears positive.

The risk level may be adversely affected by transactions executed on behalf of another person, non-transparent transactions, transfers of securities between entities from different countries, acceptance of funds from clients from risk countries (mainly tax havens and off-shore countries) or sanctioned countries. Clients with non-transparent ownership structures, sophisticated schemes, and clients having high-volume funds, whose origin may be problematic from the point of view of AML/CTF, also represent a risk.

For the purpose of reducing the risk, it is necessary that collective investment businesses apply adequately risk-oriented CDD measures and monitor and evaluate business operations through appropriately set AML/CTF scenarios.

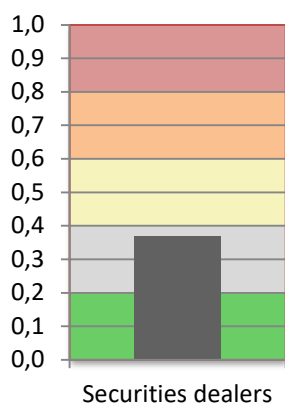
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the securities sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	AML awareness of employees
1.	Effectiveness of supervision and control activities
3.	Availability and enforcement of criminal sanctions
3.	Market pressure on compliance with AML/CTF standards
5.	Availability and enforcement of administrative sanctions
6.	Effectiveness of UTR reporting and monitoring
7.	Availability and access to BO information
8.	Availability of independent information sources

B. SECURITIES DEALERS (SECURITIES AREA)

On the basis of the evaluation of data and information obtained in connection with the activities carried out in the securities area, the ML risk was identified at the medium level - 0.37.



In particular, the fact that, compared to asset management companies, securities dealers are mainly small companies with a low number of clients, has a positive impact on the risk level. These facts therefore assume a very good (even personal) knowledge of the client's financial and property situation and the corresponding investment and risk profile of the client.

Transactions carried out in connection with an investment company's business are usually in the form of non-cash transactions, through client's payment accounts. In this way, consistent monitoring of the investment company by securities dealers, the relevant bank or financial institution, is ensured.

The risk level is adversely affected by the same facts as for asset management companies. This means that by reducing the level of performance of CDD measures, in particular by checking the origin of funds, in identifying the purpose of transaction/business relationship and inadequate monitoring and evaluation of the signs of unusualness, the ML risk increases proportionally.

Determination of priorities in activities of relevant bodies:

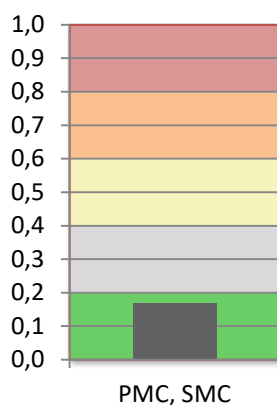
The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the securities sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of supervision and control activities
1.	AML awareness of employees
3.	Availability and enforcement of criminal sanctions
3.	Market pressure on compliance with AML/CTF standards
5.	Availability and enforcement of administrative sanctions
6.	Effectiveness of UTR reporting and monitoring

7.	Availability and access to BO information
8.	Availability of independent information sources

C. PENSION MANAGEMENT COMPANIES, SUPPLEMENTARY PENSION COMPANIES (PENSION SAVINGS AREA)

On the basis of the evaluation of data and information obtained in connection with the activities carried out in the pension savings area, the ML risk was identified at the low level - 0.17.



The fact that the saver, through his employer, pays the statutory contributions to the Social Insurance Agency and the Social Insurance Agency sends these funds to the saver's personal account in a specific PMC, has a positive impact on the risk level. Clients of businesses operating in this area are solely employees and self-employed persons registered in the Slovak Republic. In practice, there are no cash transactions with respect to pension saving contributions. Contributors are sent by the saver to their account through their employer and the Social Insurance Agency. An important fact mitigating the risk of using (misusing) products/services for ML purposes provided by pension saving businesses is the creation of right to the payment of „saved“ funds. This right is created to the client at the time of reaching a certain physical age, at which time he is also entitled to a retirement pension.

On the basis of the facts identified, it can be stated that the system of pension saving in the Slovak Republic due to its internal characteristics does not constitute an effective system of money laundering or proceeds of crime. According to the AML/CTF Act, pension saving businesses have the legal possibility to implement CDD measures in relation to the client within the scope of client identification and verification of client identification.

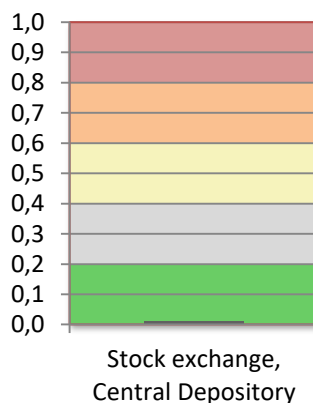
Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the securities sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of supervision and control activities
1.	AML awareness of employees
3.	Availability and enforcement of criminal sanctions
4.	Market pressure on compliance with AML/CTF standards
5.	Availability and enforcement of administrative sanctions
6.	Effectiveness of UTR reporting and monitoring
7.	Availability and access to BO information
8.	Availability of independent information sources

D. STOCK EXCHANGE AND CENTRAL DEPOSITORY

On the basis of the evaluation of data and information obtained in connection with the activities carried out by a stock exchange or central depository, the ML risk was identified at the low level - 0.02.



Due to the fact that the Slovak Stock Exchange and the Central Depository of the Slovak Republic carry out their activities primarily on a membership basis, with banks and branches

of foreign banks, securities dealers, asset management companies and other financial institutions⁶⁶, the risk of legalization almost is not present in this area.

Determination of priorities in activities of relevant bodies:

The determination of priorities is a prerequisite for effective implementation of the so-called risk-oriented approach in the activities of these authorities with direct impact on the activity of the entities. The priority was determined by assessing the impact of identified shortcomings on the activity of these entities as well as on the securities sector as a whole mainly due to its importance, character and types of activities (transactions) performed within the sector.

Priority level	Area
1.	Effectiveness of supervision and control activities
1.	AML awareness of employees
3.	Availability and enforcement of criminal sanctions
4.	Market pressure on compliance with AML/CTF standards
5.	Availability and enforcement of administrative sanctions
6.	Effectiveness of UTR reporting and monitoring
7.	Availability and access to BO information
8.	Availability of independent information sources

PART 3 - RISK OF TERRORIST FINANCING

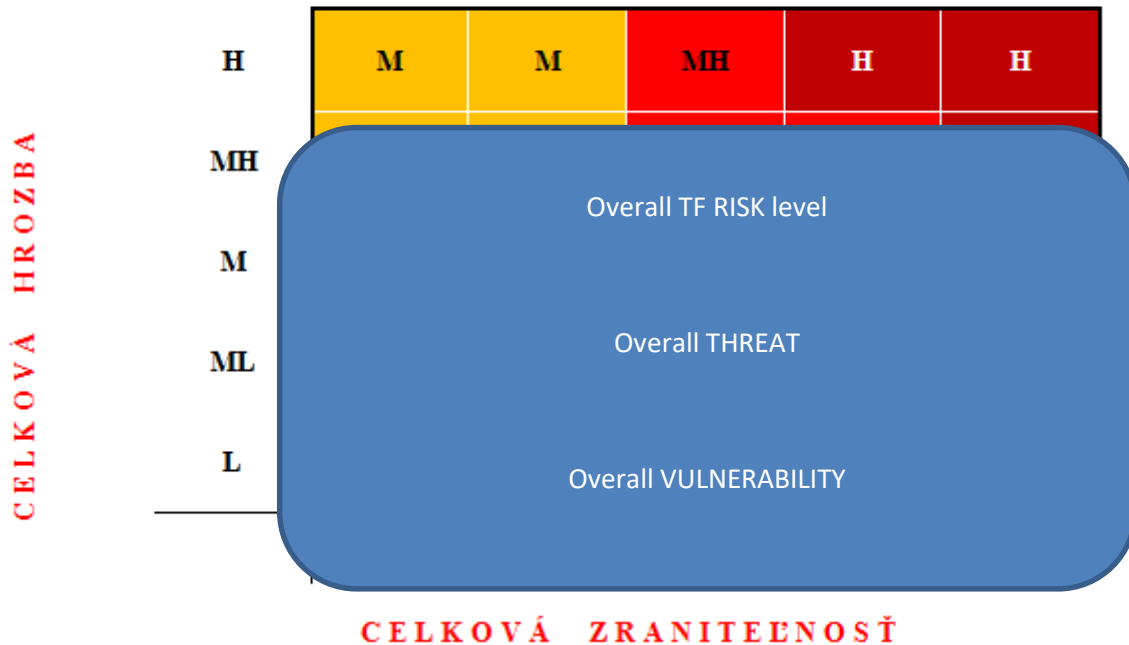
The result of the National Risk Assessment process is the identification of the overall **RISK** level of terrorist financing in the Slovak Republic is the **MEDIUM-LOW LEVEL (ML)**.

For NRA Working Party to conclude on the overall level of terrorist financing risk, it was necessary to identify the level of threats and vulnerabilities of terrorist financing at national level:

- Overall level of **THREAT** is **LOW**
- Overall level of **VULNERABILITY** is **MEDIUM-LOW**.

⁶⁶ The said businesses perform their activities based on license, or an NBS authorization and, within the meaning of the AML/CTF Act, they belong to obliged entities

CELKOVÁ ÚROVEŇ RIZIKA FINANCOVANIA TERORIZMU



3.1. THREAT OF TERRORISM IN THE CONDITIONS OF THE SLOVAK REPUBLIC

For the purpose of adequate identifying and assessing elements that positively or negatively affect the ultimate level of terrorist financing risk, it is essential as a primary step to determine the level of terrorist threat. It is a factor that determines the activities of the relevant authorities⁶⁷ in the AML/CTF area.

NATIONAL SOURCES OF TERRORIST THREAT

⁶⁷ a) The Financial Intelligence Unit NAKA P PF, b) the National Anti-Terrorist Unit NAKA P PF, c) the Slovak Information Service, d) Military Intelligence, and e) the Special Prosecutor's Office of the GPO SR provide an important contribution to combat terrorism and mainly terrorist financing.

With respect to its geographical position, size and population, the Slovak Republic is considered a smaller country, with a slight or lower impact on the global economy, international political situation and global financial systems. A relatively stable political situation, standard system of government and application of the principles of a democratic state and a positive approach to the rights of the minority population by the individual branches of public administration does not create conditions for the occurrence or formation of the groups of population that would in an extremely radical or violent manner propose or enforce their claims (e.g., related to principal changes in the state's operation).

Based on the results of the relevant authorities in the area of obtaining and evaluating knowledge and information on possible or potential security threats to the Slovak Republic and its citizens, it can be assessed that the overall threat of a terrorist attack by domestic actors was assessed as "low" in the period under review.

REGIONAL SOURCES OF TERRORIST THREATS

With respect to the geographical location of the Slovak Republic, it can be stated that neighbouring countries do not represent regional or global threat of Islamist or non-Islamist terrorism⁶⁸. These countries cannot be considered as high-risk countries or countries with serious defects in the AML/CTF system and included in the relevant FATF (Financial Action Group) list. Four of the five countries neighbouring the Slovak Republic, namely the Czech Republic, Poland, Hungary and Austria are standard EU countries, fulfilling all the tasks and conditions of membership of the integration group, particularly with regard to the implementation and transposition of EU legal acts into the national legislative. Despite these facts, a potential security threat is represented by Muslim communities in Austria (and Germany), where Salafists are exerting an increasing influence and, together with certain mosques, they can serve as a source of radicalization for both Muslims and converts. Since Slovakia is part of the Schengen zone, the free movement of radical imams operating there, which creates the possibility of radicalizing Slovak citizens in the immediate vicinity of the border as well as within the Slovak Republic, may pose a threat. Also, personal connections of some members of the Muslim community operating in Slovakia and Austria may be a potential threat. The fifth neighbouring country is Ukraine, where there is a military armed conflict. In this context, persons who have left the territory of the SR with the aim to participate in various ways in non-combat or combat activities in this area are considered a threat. In addition, Ukrainian citizens (including citizens of other countries) seeking to leave Ukraine to avoid responsibility for committing war crimes and crimes against humanity in the current conflict may also pose a risk.

Based on the results of the relevant authorities in the area of obtaining and evaluating knowledge and information on possible or potential security threats to the Slovak Republic and its citizens in the Slovak Republic, **it can be assessed that the overall threat of a terrorist attack by regional actors was assessed as "low" in the period under review.**

⁶⁸ This group includes ethnic-nationalist and separatist terrorism, left-wing and anarchist terrorism, and right-wing terrorism.

GLOBAL SOURCES OF TERRORIST THREATS

As a member of the EU and the North Atlantic Treaty Organization (NATO), Slovakia actively participates in the global fight against terrorism and is part of the so-called "EU" Counter-Terrorism Coalition in the Middle East. Public speeches by the highest government representatives of the Slovak Republic, adoption of legislative and organizational measures at national level for the purpose of supporting international efforts to fight against terrorism, tightening sentences for persons committing terrorist acts, direct participating in military and other operations, and implementing international sanctions in this area "facilitate" the designation of the SR as one of the enemies of Muslims and thus the potential target of the threat of a terrorist act or terrorism as such. There were no direct threats from globally operating Islamist terrorist groups or non-Islamist terrorist groups during the period under review. Likewise, there were no direct threats from foreign fighters or lone wolves. However, in this context, it has to be emphasized that, over the past few years, the degree of sophistication of terrorist attacks in countries belonging to the anti-terrorist coalition has been reduced, which is directly related to the cost of terrorist attacks. The most recent issue in terms of the threat of terrorism in Slovakia is the refugee crisis. The difficult economic, political, social and security situation in the countries of Africa and the Middle East has caused a massive transfer of local populations to the EU. Based on the circumstances of the entry of migrants into the EU, i.e. violent and illegal border crossing, the use of smugglers, the absence of identity documents, refusal to provide identity information, frequent use of false travel documents and identity documents, and refusal to take actions to register a person, it can be stated that **the most significant security threat is the penetration of risky persons into the European Union, secondary radicalization and lack of interest in integration in the form of acceptance, or the acceptance of the rules of conduct and cultural practices of the majority society by migrants.**

Based on the results of the relevant authorities in the area of obtaining and evaluating knowledge and information on possible or potential security threats to the Slovak Republic and its citizens in the Slovak Republic, it can be assessed that **the overall threat of a terrorist attack by global actors was assessed as "medium low" in the period under review**“.

TRANSIT AS THE SOURCE OF TERRORIST THREAT

In the period under review, despite the consistent monitoring by intelligence services, there were no cases of using the territory of the Slovak Republic as a transit country by Islamist, non-Islamist terrorist groups, or by lone wolves or foreign fighters inspired by them. There is also no route used by foreign terrorist fighters to travel to the conflict areas of Syria and Iraq. However, less sophisticated attempts to cross the EU territory with the use of the territory of the SR to travel to the conflict areas of Syria and Iraq were recorded.

Based on the results of the relevant authorities in the area of obtaining and evaluating knowledge and information on possible or potential security threats to the Slovak Republic and its citizens in the Slovak Republic, it can be assessed that **the overall threat resulting from the transit of potential terrorist offenders was assessed as "low" in the period under review.**

Overall assessment of the threat of terrorism in the Slovak Republic

Based on the above facts, measures (countermeasures) adopted by the competent authorities, the quality of legislation in the area of the application of operative as well as procedural acts, the level of national and international cooperation and last but not least the geographical location of the SR, it can be stated that the overall level of terrorist threat to the is **LOW**.

3.2. ASSESSMENT OF THE RISK OF TERRORIST FINANCING

The overall level of the threat of terrorist financing in the Slovak Republic was determined on the basis of the evaluation of the collected information and data at the **LOW** level.

The overall level of the vulnerability of terrorist financing in the Slovak Republic was determined on the basis of the evaluation of the collected information and data at the **MEDIUM-LOW** level.

The resulting level of terrorist financing risk in the Slovak Republic is at a **MEDIUM-LOW** level.

3.2.1. THREAT OF TERRORIST FINANCING

The overall level of the threat of terrorist financing in the Slovak Republic was determined on the basis of the evaluation of the collected information and data at the **LOW** level.

During the period under review, in or with respect to Slovakia, no case of terrorist financing or criminal prosecution by the Slovak law enforcement authorities regarding terrorist financing, was recorded. Also, in the framework of the investigation of suspected terrorism cases, the elements of its financing in accordance with FATF standards were not confirmed.

DETECTION AND VERIFICATION OF TERRORIST FINANCING

a) Threat of misuse of financial market products and services

The performance of the duty to report by obliged entities operating in the territory of the Slovak Republic in connection with suspicion of TF can be considered to a certain extent defensive.

The most frequently used financial market sector for the transfer of funds potentially intended for terrorist financing were **banks and branches of foreign banks operating in the Slovak Republic**.

By generalizing the information resulting from reports on unusual transactions, it can be stated that the transactions and business relations are closely monitored for TF. Transactions of entities that could be linked to countries posing a risk of Islamist and non-Islamic terrorism are examined with particular emphasis. The EU and UN sanctioning regime is strictly respected.

An example of the prudence of banks and branches of foreign banks operating in the Slovak Republic is when banks refuse to perform a transaction if the client has not adequately demonstrated a legitimate claim to crediting funds to an account, or the bank has discovered discrepancies in the client's identification documents and the submitted documents. A special category of this type was the use of false or falsified identification documents (especially foreign). The availability of a reliable identification infrastructure prevents significant misuse of such documents and potential vulnerability to terrorist

financing. At present, Slovakia has a very good and safe national identification system. A negative impact on vulnerability may have a slightly increasing trend of the use of false identity, i.e. the use of genuine identification documents in connection with the false identity of an unknown person, with the use of the similar appearance of both the persons (so-called look-a-like).

About one-third of all UTR reports were reports containing information on refusal to establish a business relationship, refusal to execute a transaction, or cancellation of a business relationship due to internal policies of banks („per internal policy“). The information provided showed the interest of persons coming from risky areas to open personal or business bank accounts, or applications for various other services, especially loans and mortgages. In some cases, the bank and the branch of a foreign bank operating in the territory of the Slovak Republic, after refusing to provide the service, also terminated the business relationship.

The following trends have been identified by analysing the individual UTR reports received during the period under review with respect to the findings and results of the analytical work of other stakeholders:

- Transfers of funds from Islamic countries, which were subsequently withdrawn in cash by the client and were intended for business purposes according to information provided by the client or for payment for goods or services, purchase of real estate, or for direct personal consumption,
- Transfers of funds from off-shore countries to persons living in the Slovak Republic and their subsequent withdrawals in cash,
- Purposeful deposits of funds in cash to personal bank accounts, whereas a natural person subsequently applies for an account statement and immediately withdraws the funds deposited.

With respect to the high degree of prudence of these institutions, the vulnerability of the banking system is relatively low.

The second most used sector of the financial market were **foreign payment institutions** providing their products and services in the area of cash transfers.

The following trends have been identified by analysing the individual UTR reports received during the period under review with respect to the findings and results of the analytical work of other stakeholders:

- With respect to the activities of foreign payment institutions in the Slovak Republic, it was found that during the period under review, the said institutions were used to transfer funds in the order of hundreds of EUR to high-risk countries such as Congo, Benin, Togo, Ghana, Uganda and Central African Republic,
- The transactions were called "help to friends". For these countries, a suspicion may arise (we cannot exclude it) that such transferred funds could subsequently be

smuggled in cash to other countries to support and finance terrorism and terrorist groups.

b) Threat of ineffectiveness of financial intelligence/intelligence

In the context of terrorist financing cases, which were examined by all legal methods and means based on

- a) Information received by the FIU based on the duty to report in respect of suspected terrorist financing, and which information was further sent to the Counter-Terrorism Department after verification,
- b) Knowledge gained through intelligence services and the Counter-Terrorism Department by their own activities,

prosecution was not initiated since all cash or non-cash transactions carried out had a real economic and legal purpose.

Likewise, no case was recorded where any crime, including organized crime, generated funds intended for terrorist financing.

Members of the Counter-Terrorism Department are authorized to obtain reports from banks and branches from foreign banks, despite the fact that such reports are subject to bank secret. They are also authorized to use information and technical means and means of operative-search activity.

In connection with the activities of SIS and MI members in the fight against the financing and promotion of terrorism, they may use legal powers, which include, in particular, information and technical means and means of operative-search activity.

c) Threat of inconsistent enforcement of international sanctions

In connection with the EU and UN sanctioning regimes, it should be noted that banks and branches of foreign banks operating in the territory of the SR consistently observed the statutory obligation to apply to the relevant central government authorities for the issue of a permit for transfer of funds to / from Iran (Council Regulation (EU) No. 267/2012 and No. 1263/2012 concerning restrictive measures against Iran). In this case, the Ministry of Finance of the Slovak Republic was responsible for ensuring the official procedure for issuing a license for the transfer of funds after the consent of other state authorities specified in the relevant provision of the Act on Implementation of International Sanctions. Based on the available information, no breaches were found by banks and branches of foreign banks operating in the SR, and it can be stated that in the area of implementation of international sanctions, cooperation at the level public sector ↔ public sector and public sector ↔ private sector is above-standard. Banks and branches of foreign banks operating in the territory of the SR also performed the duty to report and other obligations arising from the AML/CTF Act in each of the cases when the Ministry of Finance requested permission to transfer funds. There was no case (no such facts were found to justify it) of the need to propose the inclusion of a person, whether Slovak or foreign, in the sanction list.

d) Threat of misuse of non-profit organizations and public collections

In the period under review, financial and non-financial activities of non-profit organizations operating in the territory of the SR were evaluated with respect to a global trend of the misuse of publicly useful and humanitarian purposes of the establishment and activities of non-profit organizations and organization of public collections for financing terrorism. They were non-profit organizations (including public collections), whose potential for misuse to support and finance terrorism was the highest. The results showed that the funds raised were used to cover the costs of practicing faith and religious rites, promoting or providing the necessary humanitarian aid, including food product, medicines and equipment. No suspicion of terrorist financing was found, as the purpose of the funds provided was not misused. help. The purposeful use was verified without significant deviations with impact on the evaluated area.

CASH TRANSIT CONTROL

In the period under review, a total of 320 reports on cash transit were recorded at the respective border crossing points, 64 customs declarations on the average per year. A total of 37 customs declarations were submitted at international airports during the period under review. Citizens of Ukraine, the Russian Federation, Hungary and the Slovak Republic file most declarations.

Possibilities of cash transit from / to third countries in the Slovak Republic:

- 3 road border checkpoints – SR/Ukraine,
- 2 railway border checkpoints – SR/ Ukraine,
- 3 international Schengen airports.

Based on the evaluation and generalization of the information stated in the so-called single customs forms, the following customs trends in the transport of cash from / to the SR (EU) were recorded:

a) Funds on the entry to the EU:

- Purchase of transport facilities (passenger and freight) in the territory of Poland, Germany, Italy and Slovakia,
- Purchase of goods, machinery, real property;
- Account deposits;
- Personal consumption (holiday);
- Funds for business activity.

b) Funds on the exit from the EU:

- Charitable aid in Ukraine,
- Deposit for a military contingent,
- Balance (expenditure) from the purchase of transport facilities, machinery and goods.

In the period under review, the competent customs authorities imposed two block fines for not reporting the cash transit, which was subsequently detected by the luggage search. In one case, the passenger admitted cash transit upon request by a customs officer.

Increased risk of cash transit can be expected in the context of the carriage of bearer securities, jewellery, precious metals and precious stones and products made of them and

high value goods, which by their very nature are easily liquid store of value. Similarly, the increased risk can also be expected for freight transport (cargo), postal items, and possibly the transport of cash in the amount of EUR 10,000,-, which can be distributed among individual passengers.

The competent customs authorities have adequate and effective preventive and prophylactic measures in the area of cash transit control. A single reporting form was introduced during the period under review, training activities and educational activities of customs officers were intensified, awareness among the public increased through information brochures and materials at international airports. An important preventive tool was the inclusion of a specially trained service dog to search for banknotes (funds in cash). Equally, the cooperation between the respective customs authorities and the FSJ, as well as the activities of the selected FSJ officers in the examination of customs declarations, was intensified. Information from received cash transit reports is verified as part of FSJ's activities and based on the results of the analysis, the information is sent to the competent authorities in Slovakia or to FSJ's partner services abroad or entered into the FSJ internal database for further service use.

Despite the fact that, in global terms, the transit of cash to finance terrorism poses a significant threat, with respect to the individual determinants of cash transit control in Slovakia, it can be stated that the level of threat in this area is low. This statement can be supported by the following facts:

- Passengers do not carry cash in excess of EUR 10,000,-,
- Airports operating in the territory of the SR provide for the processing of fewer flights to third countries,
- The SR is a standard EU member country providing standard banking services (including a dense ATMs network allowing cash withdrawals in local currency),
- Staying in the territory of the SR does not require a significant amount of funds means to cover the necessary costs associated with staying in the Slovak Republic and the amount of consumer prices for services and goods.

THREAT OF MISUSE OF VIRTUAL CURRENCIES FOR TERRORIST FINANCING

In the period under review, the use of the virtual currency in the conditions of the SR was a matter of increasing the reputation of the entity concerned or experience. Intelligence services did not report any misuse of virtual currencies for terrorist financing in the performance of their tasks. Likewise, obliged entities did not report any suspicion of terrorist financing when verifying transactions related to the purchase and sale of virtual currencies. For this reason, the terrorist financing threat seems to be low.

With respect to further developments in the field of alternative payment systems, which are usually outside the sphere of powers of state authorities and institutions in the area of their regulation (licensing or registration), supervision and control, it is necessary to intensify cooperation and exchange of information and experience of competent authorities and pay higher attention to them.

UNIDENTIFIED FUNDS POTENTIALLY INTENDED FOR TERRORIST FINANCING

In relation to the issue of estimating the amount of funds that could be intended for funding and supporting Islamist or non-Islamist terrorism, it can be stated that in the current conditions it is not possible to quantify them accurately.

This claim can be supported by a number of factors, in particular:

- Level of terrorist threat and the threat of terrorist financing in view of the geopolitical situation in the country and the region,
- In the period under review, none dealt with the issue of terrorist financing in the SR, or scientific basis, although the issue of terrorism is generally addressed by a number of authors of publications, or students within university and university studies,
- In the period under review, no studies of economic, social and societal impact of terrorist financing on society and the national economy were prepared,
- No informal banking systems or informal payment systems (e.g. hawala), were recorded in the territory of Slovakia,
- High level of prudence of the obliged entities and the defensive performance of the duty to report.

Main reasons for the absence of scientific or theoretical knowledge in the field of terrorist financing include a lack of input data with regard to their accuracy and relevance, as their essence consists essentially of intelligence information, information subject to bank secret. Overall, the issue of terrorist financing is perceived in a sensitive way in terms of making data and information available to public sector officials, especially intelligence services, the FIU and selected Police Force units.

3.2.2. VULNERABILITY OF TERRORIST FINANCING

The overall level of the vulnerability of terrorist financing in the Slovak Republic was determined on the basis of the evaluation of the collected information and data at the **MEDIUM-LOW** level.

QUALITY OF LEGISLATION

Act No. 300/2005 Coll. Criminal Act

Current legislation includes the following elements relating to individual aspects of terrorism and terrorist financing:

- § 419 Terrorism and some forms of participation on terrorism,
- § 297 Establishing, masterminding and supporting a terrorist group,
- § 419a Participation in the combat operations of an organized armed group in the territory of another state (this concept may be used in specific cases and in the case particularly defined evidence and procedural circumstances, taking into account the purpose and sense of the criminal sanctions).

In addition, it is necessary to mention the introduced special qualification term § 140b Terrorism offenses, which means, according to the legal definition an offense under § 297 Establishing, masterminding and supporting a terrorist group, an offense under § 419 Terrorism and some forms of participation on terrorism, a crime committed by a member of a terrorist group and a crime committed based on specific motivation under § 140 e)⁶⁹.

Weaknesses:

- The issue of terrorist financing was not satisfactorily addressed under the Criminal Act and did not meet international standards in this field, in particular in relation to the funding of the so-called everyday needs of an individual terrorist⁷⁰,
- Equally, it does not reflect all international commitments of the Slovak Republic in the area, in particular a number of international conventions such as: Council of Europe Convention on the Prevention of Terrorism, including its Additional Protocol.

Negative impact on TF vulnerability: medium-low

Act No. 297/2008 Coll. on the Prevention of Legalization of Proceeds of Criminal Activity and Terrorist Financing and on Amendments and Supplements to Certain Acts as amended:

⁶⁹ § 140 e) The commission of an offense intended to commit terrorism and some forms of participation in terrorism under § 419 of the Criminal Act

⁷⁰ The deficiency was removed after repeated objections by the experts and specialists of the Council of Europe Committee MONEYVAL by Amendment No. 397/2015 dated 13.11.2015, which became effective on 01.01.2016, and partially remedied the undesired state - § 419 Terrorism and some forms of participation on terrorism. At the same time, the evaluation team acknowledged the ongoing work on amendments to the Criminal Act in connection with the transposition of the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism, which comprehensively deals with the said shortcomings

Weaknesses:

- Insufficient definition of terrorist financing (the everyday needs of an individual terrorist), which may have a negative impact on the duty to report
- Short postponement of unusual transactions,
- Absence of provision (authorization) for FIU to request the postponement of unusual transactions upon request of foreign FIU,
- Application of enhanced due diligence (EDD) to high-risk countries,
- Absence of a statutory obligation to keep statistical data on terrorist financing.

Despite the above shortcomings, in particular insufficient definition of terrorist financing and the possible impact on the duty to report, no significant weaknesses for terrorist financing were identified by analysing the reports on unusual transactions. Banks and branches of foreign banks, including payment institutions, are very prudent and consistent in examining business operations that may have any connection with terrorism, terrorist financing, as well as international sanctions. Similarly, statistical data related to TF were collected and published in the FIU Annual Report on a yearly basis, despite the absence of the statutory obligation of keeping them in the AML/CTF Act.

Negative impact on TF vulnerability: medium-low

Act No. 394/2012 Coll. on Restrictions on Cash Payments

Weaknesses:

- 2 different values for cash transactions between natural persons between each other (15,000, EUR) and between natural persons/legal entities, or legal entities/legal entities (EUR 5,000,-),
- No assessment of the impact of the introduction of a restriction on cash payments on the criminal offenses of economic nature, was performed,
- No assessment of the adequacy of the sanctions applicable and the deterrent effect of sanctions, was performed,
- Insufficient publicity and awareness of natural persons and legal entities.

Negative impact on TF vulnerability: low

Act No. 199/2004 Coll. Customs Act, as amended

Weaknesses:

- Cash checking does not cover cargo (freight transport) and postal items,
- Absence of storage of information in central electronic records,
- Unclear competences of the customs authorities in verifying the origin of funds, in temporary seizure of cash,
- Absence of closer cooperation between the FIU and the customs authorities in relation to the control of the cash transported.

Negative impact on TF vulnerability: medium-low

NBS methodological guidelines for banks and branches of foreign banks, securities dealers, insurance companies, payment institutions

Weaknesses:

- Compliance with methodological guidelines is not enforceable by the NBS; or non-compliance is not sanctionable,
- All changes in relation to AML/CTF Act are not included,
- Insufficient regulation of terrorist financing, focusing only on the execution of international sanctions in the area of funds and terrorists assets freezing.

Negative impact on TF vulnerability: low

Legislation on the activities and tasks of intelligence service

- With respect to the absence of specific SIS tasks in the **Act no. 46/1993 Coll. on the SIS** regarding terrorist financing and other aspects related to terrorism, an amendment to the Act was prepared in 2015 (effective from 1 January 2016), which extended the SIS's tasks to include acquisition, collection and evaluation of information on terrorism, including information on participation in terrorism, its funding or support, political and religious extremism, extremism manifested by violence and on harmful sectarian grouping, on activities and threats in cyberspace, if they threaten state security, and on illegal international passenger traffic and migration of persons. A significant change in the Act is also the introduction of an obligation for legal entities and natural persons who operate a website or provide a domain name. Based on a court order issued on the SIS request, the operation of a website or domain name access can be prevented if such a website or domain name disseminates ideas that promote or support terrorism, political or religious extremism, violent extremism or harmful sectarian groupings. It is one of the most important preventive tools in the fight against the spread of terrorism in cyberspace.

- Since 01.01.2016, an amendment to the **Act No. 198/1994 Coll. on Military Intelligence**, has been in force, which was explicitly expands the scope of powers of the Military Intelligence with respect to obtaining, collecting and evaluating information related to terrorism and its financing and support. The amendment was prepared in 2015.

Negative impact on TF vulnerability: low

Legislation on the implementation of international sanctions

Act 126/2011 Coll. on the implementation of international sanctions does not meet the attributes of sufficient legislation on the fight against terrorist financing. The Act does not contain administrative seizure - procedures for seizure of funds and property of sanctioned persons. Furthermore, it does not sufficiently set out the exact scope of powers and responsibilities of the relevant public administration authorities in the area of administrative seizure of funds and property of sanctioned persons. There is no precisely defined circle of persons responsible for implementing international sanctions and responsible public administration bodies, as well as their activities, duties and powers. There is an ambiguous distribution of responsibilities of public authorities in the execution of international sanctions. Plus, there is no process of the identification of natural and legal persons

endangering international peace, security and fundamental human rights, and the way they are included and excluded from in/from the list of sanctioned persons.⁷¹

Negative impact on TF vulnerability: medium

Legislation on corporations

Basic legislation governing the formation and operation of corporations:

a) Act No. 213/1997 Coll. on non-profit organisations providing welfare services⁷², as amended.

In order to achieve the highest possible degree of transparency with regard to the use of funds for the tasks and activities of non-profit organisations, they are required to keep accounts and prepare annual financial statements. In special cases, the annual financial statements need to be audited. In accounting, they are obliged to keep separately revenues and costs associated with welfare services and the revenues and costs of their business. The audited annual financial statements are published in the Trade Journal.

Non-profit organizations are also obliged to prepare an annual report containing an overview of activities carried out in the calendar year, showing the relationship to the purpose of establishing a non-profit organization, the annual financial statements and the assessment of the underlying data, an overview of cash revenues and costs, an overview of the revenues broken down by resources, status and movement of assets and liabilities of a non-profit organization, and others.

b) Act No. 34/2002 Coll. on Foundations and on amendment to the Civil Code, as amended,

In order to achieve the highest possible degree of transparency with regard to the use of funds for the tasks and activities of foundations, they are required to keep accounts and prepare annual financial statements. In special cases, the annual financial statements need to be audited.

Foundations are required to prepare an annual report that is publicly available. This includes, inter alia, an overview of the activities carried out, an overview of revenue by source and origin, an overview of donors, an overview of the natural and legal persons to whom the foundation has provided funds and the way they were used, expenditure by activity type and others.

⁷¹ The Act was effective in the period under review. On 15 November 2016, a new Act no. 289/2016 Coll. on the implementation of international sanctions became effective, which largely eliminated all identified shortcomings related to the implementation of FATF international standards.

⁷² Welfare services: provision of health care, provision of social assistance and humanitarian care, creation, development, protection, restoration and presentation of spiritual and cultural values, protection of human rights and fundamental freedoms, education, education and development of physical culture, research, development, technical-scientific services and information services, creation and protection of environment and protection of public health, services to support regional development and employment, provision of housing, administration, maintenance and restoration of housing stock.

c) Act No. 147/1997 Coll. on Non-Investment Funds and on Changing and Amending the Act of the National Council of the Slovak Republic No. 207/1996 Coll., as amended.

In order to achieve the highest possible degree of transparency with regard to the use of funds for the tasks and activities of non-investment funds, they are required to keep accounts and prepare annual financial statements. In special cases, the annual financial statements need to be audited.

Non-investment funds are obliged to prepare an annual report that is publicly available. This includes, among other things, an overview of the activities carried out, an overview of donations and contributions, an overview of revenue by source and its origin, expenditure by activity type and others.

d) Act No. 162/2014 Coll. on public collection, and amending and supplementing certain laws

In order to achieve the highest possible degree of transparency with regard to the organization of public collections, the entities concerned are obliged to submit and publish the following documents:

- Interim report on the collection containing a collection overview, gross revenue overview by collection methods, and bank account statements from a special account,
- Final report on the collection, containing an overview of the costs of the collection and an overview and evidence of the use of the collection's net proceeds for its purposes.

The purpose of the public collection is clearly defined by that law, it is a generally beneficial purpose⁷³ or for individually specified humanitarian aid for a natural person or a group of natural persons in distress, at risk of life or in need of emergency assistance in case of a natural disaster.

Negative impact on TF vulnerability: low

QUALITY OF INTELLIGENCE INFORMATION

The success of the fight against terrorist financing is conditional on early identification of suspicious activities and effective and flexible cooperation between security forces as well as the exchange of real-time intelligence. In the period under review, the quality of intelligence is assessed as sufficient/optimal. The fact that no prosecution was initiated is a proof of the above stated TF threat, i.e. the national coordination mechanism and the preventive measures taken by obliged entities and competent authorities are at a sufficient level.

⁷³ Generally beneficial purpose: development and protection of spiritual values; protection of human rights; protection and creation of the environment; preservation of natural and cultural values; health protection; social services development; development of education and physical fitness, development of volunteering, development cooperation and humanitarian aid, defence of the rights of disadvantaged groups of natural persons, and support for work with children.

On 1 January 2013, the National Security and Analytical Centre (NBAC), included in the organizational structure of the SIS, was established to streamline the cooperation between security forces. The NBAC represents a new form of interdepartmental organizational structure in the form of a joint centre, bringing together at national level the bodies competent in the CTF area and serious security threats to the SR, its citizens and interests. NBAC is defined as an analytical, communication and collaborative workplace of SIS with the nationwide coverage for security threats. Key tasks of NBAC include the preparation of comprehensive analytical assessments of security incidents based on reports and statements received from public authorities of the Slovak Republic, monitoring of the security situation in the Slovak Republic in uncovered sources and provision of analytical products on security threats in the SR to designated recipients. The basic philosophy of NBAC's activity is to develop a wide analytical centre based on active participation of Slovak public authorities operating in the security field in Slovakia (SIS, MI, PF, KUFS, Ministry of Foreign and European Affairs) by sending their representatives to NBAC.

In order to propose an appropriate effective way of exchanging operational information under the current legislation on entities suspected of organized crime, money laundering and terrorist financing, coordinating activities related to the detection and documenting of criminal group crime to avoid duplicate activities in dealing with individual cases and on natural and legal persons suspected of money laundering or terrorist financing, the MISO-LP was established within the MEKO. Members: PF, SIS, NBS, FD SR, MoF SR, MI, MoJ SR, GPO SR, MoE SR, Academy of the Police Force in Bratislava.

Weaknesses: irregular intervals of meetings, insufficient orientation on TF issues, some ministries do not respect the conclusions and tasks resulting from the negotiations, MISO-LP as such has a weak position, conclusions and decisions are not constitutive (binding), weak enforcement of tasks performance, weak personnel and organizational support for the performance of MISO-LP's tasks concerning the scope of activities and focus.

EFFICIENCY OF THE SYSTEM OF REPORTING UNUSUAL TRANSACTIONS RELATED TO THE TERRORIST FINANCING, MONITORING AND ANALYSIS

During the period under review, FSJ received UTR reports as provided below, with suspected terrorist financing. The subsequent analysis of the information contained in individual reports is one of FSJ's key tasks. In justified cases, the results of the analysis are sent in the form of "FSJ products" to the competent Police Force department - Counter-Terrorism Department⁷⁴. In principle, FSJ products contain processed relevant information stated in UTR reports, including additional facts relevant to the further operation of the Department. It is, in particular, information obtained from other obliged entities who had relevant information at the time of the examination. Partner foreign financial intelligence units are also requested to cooperate, if necessary.

⁷⁴ Starting from 1 February 2017 - the National Anti-Terrorist Department of the National Criminal Agency of the Police Force Presidium

Year	Number of UTR reports received	Number of FSJ products sent to the Counter-Terrorism Department
2011	103	103
2012	112	112
2013	86	86
2014	79	79
2015	83	83

The above statistical data demonstrate the efforts of obliged entities to thoroughly verify the transactions of their clients and the results of the analytical activities of FSJ. Given the characteristics of the SR in terms of the threat of terrorism and terrorist financing, the information provided in this way is valuable and usable, but the elements of the suspected terrorist financing were not confirmed by the other departments.

Negative impact on vulnerability: medium-low

ADEQUACY OF RESOURCES

Considering the risk and size of the country in relation to terrorist financing, almost all competent authorities consider their staffing, technical and organizational resources to be adequate to take appropriate countermeasures.

However, in view of its legal status as a central national unit in the area of prevention and detection of money laundering and terrorist financing, FSJ has been understaffed in the long term. Resources allocated to FSJ are disproportionate to the seriousness of the issue and do not fundamentally reflect its current needs. The lack of strategic and operational concept of the activity is due to the high rate of fluctuation of its managers.

Negative impact on vulnerability: medium-low

EFFICIENCY OF INTERNATIONAL COOPERATION

a) Legal basis for international cooperation

From the point of view of the authorities that play a significant role in the fight against terrorism and terrorist financing, no shortcomings or weaknesses of legislation with respect to the performance of formal international cooperation, were identified.

Significant legal instruments and concept for fighting against TF:

- AML/CTF Act empowers FIU members to conduct international cooperation (FIU-FIU) directly, without the need to conclude Agreements on Mutual Understanding, which makes

it possible to reduce the bureaucratic burden; in practice, international cooperation can be organized immediately, which is positive in terms of time. However, for the exchange of information between FIU-FIU, the so-called Egmont principles of information exchange must be applied.

Year	FIU's request	Request from abroad
2011	14	4
2012	1	14
2013	0	0
2014	0	0
2015	0	5

- The Joint Investigation Team – JIT and the Joint Customs Operations – JCO are institutes that can be used by the National Counter-Terrorism Department to fight against TF according to the current legislation. However, during the period under review, such an institute was not used, because no direct activity by terrorist groups has been reported so far, or no persons or groups preparing to commit a terrorist offense were localized.

- Mutual cooperation and exchange of information within the intelligence community is adequately regulated in the relevant legal regulations regulating the activities and position of intelligence services operating in the SR. International cooperation is based on a multilateral and bilateral exchange of knowledge, assessments and analyses.

Negative impact on vulnerability: low

b) Judicial cooperation

No request for international legal assistance related specifically to TF was received in Slovakia in the period under review. However, if such a request is received, it would be handled with the highest priority. There are no legal barriers in the Slovak system of law preventing the performance of the widest possible range of required acts, including seizure and coercive measures interfering with fundamental human rights and freedoms.

In the period under review, the SR did not send any request for international legal assistance in connection with TF.

In the period under review, Slovak authorities processed four requests for international legal assistance (two with respect to a terrorist offense motivated ideologically by so-called left-wing terrorism and two with respect to terrorist attacks related to Islamist terrorism).

Negative impact on vulnerability: low

c) International police cooperation⁷⁵

When evaluating statistical data in the context of the scope of international police cooperation, it should be stressed that the requests received or sent were broad in terms of the information requested, and in principle covered both terrorism and terrorist financing.

Year	Requests received	Requests sent
2011	232	82
2012	463	230
2013	0	0
2014	120	47
2015	583	136

Negative impact on vulnerability: low

d) Informal cooperation

The use of informal cooperation is only possible in the context of unclassified information for the purpose of processing the request more quickly, sending information or for the purpose of bridging technical issues. Due to the sensitivity of information and the potential for information leakage, such a form of cooperation should be carefully considered.

Due to the lack of its own experience (cases), Slovakia cannot actively engage in the activities of various working groups assessing TF risk at the global level, or in the preparation of indicators. This fact may result in a deterioration in the reputation of the competent Slovak authorities from the point of view of partner bodies and institutions.

Negative impact on vulnerability: medium-low

AWARENESS AND INVOLVEMENT IN FIGHT AGAINST TERRORIST FINANCING

Terrorist financing is a horizontal problem, which at first sight seems to pose a challenge not only to intelligence services, relevant police bodies, including FSJ, but also to prosecutors' offices, and also due to its complexity interferes with the roles and activities of various other government authorities such as the MoJ SR, Ministry of Foreign and European Affairs, FACO, MoF SR, MoE SR and others.

The result of political involvement in the fight against terrorist financing is the publication of the "Strategic plan to Combat Money Laundering and Terrorist Financing for the years 2012-2016" by the Police Force Presidium. It was a strategic document that, in an

⁷⁵ Statistical data represent a summary of executed international police cooperation carried out by national INTERPOL Bureau and national EUROPOL Bureau.

aggregated form, provided insight into the legislative, organizational, institutional arrangements of the ML and TF system at national level. The document also includes the results of operational and strategic analyses based on reports on unusual transactions in the form of the most commonly used methods and forms of ML and TF. Its implementation resulted in practical changes in the system.

Another strategic document is the National Counter-Terrorism Action Plan, its main tasks include to create an appropriate environment for the follow-up of international commitments, such as bilateral and multilateral agreements, UNSC resolutions, decisions and resolutions of EU institutions or sanctions of international institutions against persons and entities associated with terrorism. Its main purpose is to contribute to higher security of Slovak citizens and readiness of public authorities in the event of a terrorist attack on the territory of the SR.

The result of a high level of awareness among the main actors in the fight against terrorism is the implementation of international conventions, relevant FATF Recommendations (FATF Special Recommendations) in Slovak law and the preparation of public and non-public guidelines for obliged entities.

Negative impact on vulnerability: low

GEOGRAPHIC AND DEMOGRAPHIC FACTORS

a) Geographical factors

Open borders within the EU and the resulting freedom of movement of persons within the Schengen area pose a potential threat in the form of uncontrolled flows of migrants, including those with a criminal background, who were prosecuted in the past, as well as have experience in fighting in crisis areas.

Weaknesses: There is a threat of using the SR as a background for undetected logistic activity for the needs of terrorist financing/obtaining funds for its financing; the deterioration of the security situation from the point of view of Islamist radicalization in neighbouring countries (especially Austria).

Negative impact on vulnerability: medium

b) Demographic factors

There are no risk groups of inhabitants in Slovakia. The Muslim community operating in the territory of the Slovak Republic presents itself as moderate, its representatives have long avoided radical manifestation and expressions about the activities of Islamists in conflict zones.

Weaknesses: The possibility of radicalization, especially of the younger generation of the Muslim community, through radical Islamic materials freely available on the Internet, as well as through foreign clerics visiting and lecturing in Slovak prayer houses.

Negative impact on vulnerability: low

OTHER FACTORS

For the purpose of assessing all potential vulnerabilities in terms of terrorist financing, the following areas were identified as determinants:

a) Corporations⁷⁶

With respect to the performance of statutory tasks in the fight against terrorism, including the fight against terrorist financing, the competent authorities did not report any misuse of non-profit organizations operating in the territory of the SR for the purpose of terrorist financing or obtaining other than financial support for terrorist groups; regardless of whether it was funding for Islamist or non-Islamist terrorist groups.

With respect to the performance of tasks by FSJ in the conduct of controls in a corporation aimed at verifying the purpose of disposal of property, no facts were detected that would confirm a suspicion of TF. Likewise, in performing statutory tasks, in the period under review, they did not receive or verify any UTR report by which a bank or branch of a foreign bank reported the fact that a corporation whose payment account is administered with the relevant bank or branch of a foreign bank, performed debit transactions or had credit transactions suspected of TF.

From the point of view of the activities of the relevant public authorities, the quality of the legislative measures and the activities of the obliged entities linked to the activity of corporations, it is possible to state **a medium-low level of negative impact** on the vulnerability of the CTF system.

b) Exchange activity

In Slovakia, foreign exchange activity is carried out by two types of businesses:

- a) Banks and branches of foreign banks,
- b) Exchange offices based on the foreign exchange license issued by the NBS,

In connection with FSJ's tasks in the control of exchange offices for the verification of the purpose of the disposal of assets, no facts were found that confirmed the suspicion of TF.

In the period under review, when performing statutory tasks, FSJ did not receive and review any reports on unusual transactions through which a bank and branch of a foreign bank announced the fact that terrorist financing was suspected in the provision of exchange services. Similarly, no reports on unusual transactions were received from the exchange offices that the conduct of their client/client indicate that the execution of the transaction could result in terrorist financing.

⁷⁶ Corporation shall mean, under the AML/CTF Act: a) a foundation, b) a non-profit organization providing generally useful services, c) non-investment fund or d) another special-purpose corporation irrespective of its legal personality which manages and distributes funds.

From the point of view of the activities of the relevant public authorities, the quality of the legislative measures and the activities of the obliged entities, it is possible to state **a medium-low level of negative impact** on the vulnerability of the CTF system.

c) Financial inclusion products

During the period under review or at the time of providing the basic banking product by banks and branches of foreign banks they did not report to FSJ any suspicion of terrorist financing for which the basic banking product would be misused.

Based on the assessment of the measures taken by banks and branches of foreign banks in relation to the basic banking product, it can be stated that the measures taken are appropriate for the risk of the product. The scope of the customer due diligence is applied to the same extent as with other clients of banks or branches of foreign banks, in particular by using the "KYC" - "Know Your Customer" principle, established monitoring mechanisms to detect unusual or suspicious transactions. In fact, banks and branches of foreign banks do not differentiate current account clients and clients with basic banking products and treat them equally.

A limiting factor in the possibility of TF through the basic banking product is the statutory maximum annual turnover on the account. This fact, together with consistent application of customer due diligence (CDD) by banks and foreign bank branches and the low preference of this product by their clients, results in a **low level** of vulnerability of financial inclusion products in the Slovak Republic.