COMMITTEE OF EXPERTS ON THE EVALUATION
OF ANTI-MONEY LAUNDERING MEASURES AND
THE FINANCING OF TERRORISM (MONEYVAL)

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

MONEYVAL(2020)21

Anti-money laundering and counter-terrorist financing measures

Slovak Republic

Fifth Round Mutual Evaluation Report

September 2020

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems. Through a dynamic process of mutual evaluations, peer review and regular follow-up of its reports, MONEYVAL aims to improve the capacities of national authorities to fight money laundering and the financing of terrorism more effectively.

The fifth round mutual evaluation report on Slovak Republic was adopted by the MONEYVAL Committee at its 60th Plenary Session

(Strasbourg, 16 – 18 September 2020).

Contents

EXECUTIVE SUMMARY

1. This report summarizes the anti-money laundering counter financing of terrorism (AML/CFT) measures in place in Slovak Republic as at the date of the on-site visit from 7-18 October 2019. It analyses the level of compliance with the Financial Action Task Force (FATF) 40 Recommendations and the level of effectiveness of Slovak Republic's AML/CFT system and provides recommendations on how the system could be strengthened.

Key Findings

1. The first National Risk Assessment (NRA) of Slovakia was officially acknowledged by the Government in 2019, with a significant time lag between the data used and the publication of the report. The assessment team (AT) has some concerns about the accuracy of the NRA's findings given that: certain risks (including the use of fictitious companies, the Fintech sector, the use of cash and external threats), have not received a significant attention; and the NRA provides a limited description of the main money laundering (ML) methods, trends and typologies. The assessment of terrorism financing (TF) risks is an area for improvement. In case of supervisory authorities, the understanding of ML/TF risks is also based to some extent on the results of supervisory activities, information exchange with foreign supervisory authorities, supra-national risk assessment conducted by the EU, and in case of the FIU the number and the content of the UTRs. The LEA's understanding of risk is based on practice and on the GPO's sectoral vulnerabilities assessment.

2. While some of the prosecutors have a more accurate understanding of ML threats which include organised crime (OC), corruption and cybercrimes, the rest of law enforcement agencies (LEA), supervisors and the private sector, are grounding their knowledge on the findings of the NRA.

3. The LEAs making more use of the financial intelligence are the Financial Police Unit NAKA and ARO NAKA while the use of financial intelligence by other Police Forces is minimal. The absence of a bank account register, together with the lack of BO register were reported as the greatest challenges in conducting financial analysis. While there are some positive results, overall, the FIU products are not successfully utilised by LEA in ML cases. SR has weak results both in terms of ML investigations conducted based on FIU disseminations, and, more generally, in using financial intelligence and other relevant information to develop evidence and trace criminal proceeds related to ML However, LEA have exploited the FIU's intelligence packages for investigations into predicate crimes.

4. The financial intelligence unit (FIU) officers are knowledgeable and have the ability of producing complex analysis, but for most of the evaluation period there was insufficient coherence in the competent management to gear their activities into becoming effective. One of the important shortcomings lays with the FIU's dissemination system which dissipates its resources into less relevant cases, often not related to ML. This has a negative impact on the quality of the analysis and bares repercussions on the reporting entities (RE) appetite to report.

5. Overall, the FIU receives a reasonable number of unusual transactions reports (UTRs) although their quality varies. Recently the FIU started to improve the feedback given to the RE. On a less positive side, the process of prioritisation of UTRs seems to be inefficient, with almost 90% of the reports placed under the higher risk categories.

6. The ML offences are identified and investigated by the authority having competence over the predicate offence. The assessors note that LEAs collect information on predicate crimes

in the operative pre-investigative proceedings but do not appear to pay due attention to the identification of proceeds and to associated ML activities. It appears to be lack of timeframes and insufficient monitoring in the investigative stage which leads to lengthy proceedings.

7. Since 2013 the number of ML convictions increased to an overall number of 91, an important part pertaining to simple property crimes such as car thefts. The outcome of investigations and prosecutions of ML in other major proceeds generating offences do not fully reflect the country's risks.

8. The effectiveness of the provisional measures applied in financial investigations is seriously affected by the lack of proceeds-oriented operative analysis in the pre-investigative proceedings, the logistical and procedural constraints at certain LEAs, the (putative) limitations to seize assets from third parties, and the high evidentiary burden required for certain provisional measures.

9. The confiscation measures are rarely if at all imposed in criminal cases and only a fragment of the secured assets will finally be confiscated.

10. There have been no TF convictions in the assessed period. Three relatively complex TF investigations are currently being conducted by the Counter-Terrorism Unit NAKA (CTU-NAKA), and demonstrate both the applicability of the legal framework and the ability of the Slovak authorities to detect potential TF cases and to effectively cooperate with their foreign counterparts.

11. The Ministry of Foreign Affairs (MFA) has the clear role to communicate the potential targeted financial sanctions (TFS) proposals to United Nations (UN) Committees, although has a limited role in the designation itself. There are no clear regulatory instructions in the designation process and there is a risk that the authorities would rely on each other to make a designation if the case may occur. No assets have been frozen pursuant to TFS UN Security Council Resolutions (UNSCRs), and no instances of *"false positives"* have been reported.

12. The NRA sees the non-profit organisations' (NPOs) exposure to FT abuse as low, but no specific types of more vulnerable NPOs have been identified. Slovak Information Service (SIS) and CTU-NAKA perform regular supervision over certain NPOs, but this appears to be done more on case-by-case basis than systematically.

13. Banks demonstrated a good understanding of the ML/FT risks, but some non-bank financial institutions (FIs) (money and value transfer service (MVTS) providers and exchange offices) and designated non-financial businesses and professions (DNFBPs) were unable to clearly articulate how ML might occur within their institution or sector. FIs and DNFBPs were less confident in their understanding in relation to FT risk and did not demonstrate sufficient understanding of FT threats and vulnerabilities.

14. Banks and most non-bank FIs demonstrated knowledge of the AML/CFT requirements including an adequate application of basic customer due diligence and record-keeping requirements, although some common gaps persist. DNFBPs have a moderate understanding of the preventive measures. There remain concerns regarding the procedures applied for the verification of BOs of legal entities.

15. While the FIs and DNFBPs generally understand the procedures for reporting, most non-bank FIs and DNFBPs were unable to elaborate on typologies, transactions or activities that would give rise to a UTR, particularly in relation to TF.

16. The scope and the depth of inspections conducted by the FIU and the NBS are not fully

risk based. The reason behind is the lack of a documented process in place, which sets out how subject person specific ML/FT risk-ratings drive the frequency, the scope and the nature of future supervisory onsite/offsite inspections, as well as the lack of resources available for AML/CFT supervision.

17. Slovakia created the "Register of legal entities, entrepreneurs and public authorities" (hereafter the UBO register) in 2018. At the time of the onsite, the register was still being populated (only 12 % of legal persons had inserted their UBO data into the UBO register), though the filling in of the register progressively continues. There are no mechanisms in place to verify the information on the UBOs at the time of registration. Some control mechanisms are done *ex post* by state authorities, such as LEAs, tax authorities, as well as by media and NGOs.

18. Besides the UBO register, the Register of Public Partners also contains information on UBOs of legal entities involved in public procurement. The state authorities and private sector consider the data contained in this register as high quality. Although there is a system of verification, the UBO information is mainly identified and verified by some DNFBPs who have a formal and limited understanding of UBO.

19. Authorities have generally been active in providing mutual legal assistance (MLA) in relation to foreign requests in a constructive and timely manner, which also goes for requests related to the seizure of property as well as the participation in numerous joint investigation teams (JITs). At the international level the FIU is active and responsive and the feedback provided by the international community was generally positive.

Risks and General Situation

2. The level of various forms of economic crime remains a key ML vulnerability of the country. According to the NRA statistics on reported crimes, the offences generating the highest damage are frauds in various forms (credit, tax), theft, embezzlement, tax and insurance evasion, and failure to pay tax and insurance. The overall level of the TF threats in Slovakia was rated by the NRA as *"low"*. The conclusion is mostly based on the absence of terrorist acts in Slovakia and in the neighbouring countries as well as the geographical position of the country which minimizes the threat of cross-border cash transfers for TF purposes. The TF vulnerability is assessed as *"medium-low"* resulting in an overall *"medium-low"* TF risk.

3. SR is not a major international financial centre. The Slovakian economy has shown a positive economic trend over the last number of years. The tertiary, services sector, dominated by trade and real estate, contributes to 55.94% of gross domestic product (GDP) and employs around 60.8% of the workforce. The secondary, industrial sector is the second important contributor to economy, employing 36,07% of the workforce and representing 30.97% of GDP.

4. The banking sector accounts for more than 70% of total financial sector assets in 2018; insurances (7.14%) and investment funds (7.13%) come next.[1] As of 2018, there are 12 Slovak and 15 non-Slovak European Union (EU) banks registered, as well as 14 Slovak and 21 non-Slovak (EU) insurance companies registered together with 40 securities companies. From the 12 Slovak banks, 8 have foreign ownership worth more than 50% and the remaining 4 banks have 100% resident shareholders. The value of assets maintained in the latter 4 banks is almost 6 times higher than for the 8 foreign ownership banks.

Overall Level of Compliance and Effectiveness

[1] Annual report of the NBS, 2018

5. Slovakia has taken some significant steps in strengthening its AML/CFT framework since its last evaluation, most notably by undertaking NRA, changes in the Police Force structure and with the enactment of the International Sanctions Act (ISA) in 2016. In some respects, the elements of an effective AML/CFT system are in place but in several aspects, the framework is relatively new and therefore it has not been possible to demonstrate the overall effectiveness of the system. The exception to this is that international cooperation is taking place effectively at a large extent. Generally, major and fundamental improvements are needed to demonstrate that the system cannot be used for ML/TF and the financing of proliferation of weapons of mass destruction.

6. In terms of technical compliance, the legal framework has been enhanced in several aspects such as transparency of legal persons and arrangements. Nevertheless, a number of issues remain including customer due diligence (R10), suspicious transactions reporting (R20), higher risk countries (R.19), and the analysis function of the FIU (R.29).

Assessment of risk, coordination and policy setting (Chapter 2; IO.1, R.1, 2, 33 & 34)

7. The NRA was approved by the Government in May 2019. The document addresses both ML and FT risks and includes the assessment of threats and vulnerabilities. The AT has some concerns in relation to the accuracy and reasonableness of the conclusions of the NRA in two major points: i) the time gap between the statistical data used and the moment of the adoption of the report, ii) certain risks (including the use of fictitious companies, the Fintech sector, the use of cash and external threats), have not received a significant attention and iii) the NRA does not provide a comprehensive description of the main ML methods, trends and typologies. The national statistics system was considered as a limiting factor in the work of the NRA task force with other evidence of inefficient data management.

8. The main document adopted to address the identified ML/TF risks is the "Action plan for combating money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction for the period 2019 – 2022" (hereafter AP). The AP contains a broad list of measures to be taken by the relevant authorities to address the vulnerabilities identified in the NRA, such as: introduction of proactive parallel financial investigations in ML cases; organization of trainings and workshops for the FIU; raising awareness of obliged entities on their AML/CFT obligations through training and methodological documents; enhancing the comprehensiveness of statistics kept by the FIU; updating the NRA; development of typologies of more sophisticated ML schemes using of legal entities, cross-border operation and implication of tax havens etc… As described under CI1.1, the AP is of a moderate help for the authorities in addressing the risks. Some of the orders and recommendations are more general and do not have a direct applicability in practice, while others are easier quantifiable in terms of results.

9. When applying the CDD measures, the REs are required to consider the risks, including those identified at the national level. Overall, the AT found that the results of the NRA were not always used for revising the ML/TF risk assessments by the private sector, but the conclusions on the country risks prepared by the individual RE (especially larger financial institutions) were relatively consistent with the NRA and tended to be even more accurate and detailed than the NRA.

10. The Interdepartmental Expert Coordination Body on Combating Crime (MEKO), is the long-established group for strategic coordination between relevant authorities which demonstrated its effectiveness in coordinating the development and implementation of policies and activities to combat ML/TF. Under the coordination of the Ministry of Interior (MoI), the following authorities are part of the MEKO: the General Prosecutor's Office (GPO), SIS, Police

Forces, the Court Guards and Prison Wardens Corps, the Military Police Military Intelligence; the Department of Fight against Frauds of the Financial Directorate; Financial Administration Criminal Office (FACO), the Ministry of Justice (MoJ), the Customs Department, and Civil Aviation Section of the Ministry of Transport and Construction.

11. The FIU and the NBS have communicated the outcomes of the NRA to the financial institutions (FIs) and designated non-financial business and professions (DNFBPs) by conducting awareness-raising meetings and trainings and by publicising the NRA on their websites. However, outside the content of the NRA itself, the authorities did not provide risk models or further risk guidance to the supervised entities. Private sector stakeholders are generally informed about AML/CFT risks.

Financial intelligence, ML investigations, prosecutions and confiscation (Chapter 3; IO.6, 7, 8; R.1, 3, 4, 29–32)

12. Financial intelligence is generated by the FIU, which was situated within the NAKA during most of the evaluation period. Both the FIU and the LEA have access to a wide range of administrative, law enforcement and financial information sources. The FIU regularly seeks and obtains information to conduct its analysis. The authorities are unanimous in saying that the private sector's reporting on TF is adequate and the number of UTRs does not pose a significant burden on the FIU work.

13. Intelligence generated by the FIU has a limited value for the PF which only occasionally used it in ML investigations. The analysis process of the FIU generally consisted in linking incoming UTRs with existing ones and seeking information from databases and other domestic and foreign authorities to determine the suspect's economic profile and establish a link to an underlying criminal activity. There are several elements undermining the FIU effectiveness the most prominent being the insufficiently coherent and stable management and dysfunctional dissemination mechanism.

14. The AT does not see any impediments encountered by LEA or FIU in accessing financial intelligence and other information to develop evidence and trace criminal proceedings and ML. The limited results in this regard, appear to be caused more by an absence of LEAs awareness and capacities (including specialised human resources and guidance) in exploiting the financial information rather than shortage of legal means and/or opportunities.

15. Overall, ML is not sufficiently detected and investigated by LEA regarding suspicion arising from UTRs, identified by financial institutions and DNFBPs, or by systematically harvesting financial information in proceeds generating cases. Parallel financial investigations are conducted but not systematically and not in all cases where the associated predicate offences occur.

16. The authorities have prosecuted all types of ML cases, including self-laundering, third party laundering and stand-alone ML. However, the investigations and prosecutions of ML is not fully in line with the risks faced by the SR, as they are overly focused on domestic crime predominantly theft or frauds of relatively low profile.

17. The centrepiece of the confiscation regime is the forfeiture of property which, however, was not convincingly demonstrated to guarantee the actual deprivation of criminal proceeds and its success is heavily dependent on the effectiveness of the provisional measures applied in financial investigations.

18. The latter are seriously affected by the lack of proceeds-oriented operative analysis in the pre-investigative proceedings, the logistical and procedural constraints at certain LEAs, the limitations to seize assets from third parties, and the high evidentiary burden required for

certain provisional measures. Even if the statistical figures for seizures can illustrate the capability of the regime to reach various sorts of assets in remarkable volume, the SR has yet to demonstrate what proportion of criminal proceeds secured in the investigative stage has finally been confiscated by the courts as well as the value of the confiscated property that has been effectively recovered.

19. There are some procedures, but no comprehensive mechanism for the managing and/or disposing of property that is seized or confiscated and neither is there any centralized body in charge of the management of such property, bearing a direct impact on effectiveness, particularly if more complex types of assets have to be managed. The cross-border cash control regime has not demonstrated its effective ability to detect ML/TF potentially related to cash/BNIs transported through the borders of the SR that also constitute external borders of the EU. In the few cases of false or non-declaration, no assets were restrained and there is no mechanism available to counter cash couriers entering through the EU internal borders.

Terrorist and proliferation financing (Chapter 4; IO.9, 10, 11; R. 1, 4, 5–8, 30, 31 & 39.)

20. The NRA identifies the TF risk in Slovakia as *"medium-low"* due to several factors such as country's geographical location, its population profile and its economy. Nevertheless, there are some shortcomings in relation to the accuracy and completeness of the NRA, with some potential TF risks not being fully addressed. (e.g. poor control on the cash movements across the country; money remittances, as well as the use of fictitious corporate structures; non-dissuasive nature of sanctions in relation to undeclared/falsely declared movement of cash, etc.).

21. There have been no TF convictions in the assessed period. Three relatively complex TF investigations are currently conducted by the Counter-Terrorism Unit NAKA. The TF investigations introduced to the assessors appear to demonstrate both the applicability of the legal framework and the ability of the Slovak authorities to detect potential TF cases and to effectively cooperate with their foreign counterparts.

22. In the assessed period, a total of 464 UTRs have been sent to the responsible LEA Unit, namely the Fight Against Terrorism Unit of the Police Force Presidium (until 2016) and Counter-Terrorism Unit – NAKA (after 2016). The FIU filters some 20% of the UTRs, the rest being disseminated to LEA.

23. As a member of the EU, Slovak Republic applies the EU legislation for the implementation of TFS. At the national level, the International Sanctions Act (ISA) creates a system for the Government to declare an international sanction if need occurs. The Ministry of Foreign Affairs (MFA) is the authority responsible for submitting a designation request to the relevant UNSC Committee through the Permanent Representation of the SR to the UN. However, the ISA establishes a vague designation procedure, making reference to a *"responsible authority"* which can be any state body in Slovakia[2].

24. To date, the SR has not proposed or made any designations and there have been no freezing under UNSCRs 1267 and 1373. The REs and competent authorities have at their disposal legal mechanisms and instruments for applying freezing measures as described under the TCA. Most of the financial sector is aware of the TF obligations and have a good

[2] The NAKA, the Financial Administration Criminal Office, the Military Intelligence, the Office of Criminal Police, the FIU, the MoF, the MoI, the MoD, the MoJ, the MFA, the Ministry of Transport, the Ministry of Labour, the Ministry of Environment, the Ministry of Education, the Ministry of Culture, the Ministry of Soil Management, the Ministry of Health Care, the Ministry of Construction.

understanding of their freezing and reporting obligations. FIs mostly use commercial databases or have developed their own integrated screening systems to check clients and to automatically update the sanction lists.

25. The NRA looked at the NPOs operating in the territory of the SR with respect to a global trend of the potential misuse. The assessment is rather superficial and concluded that there are NPOs (including public collections), whose potential for misuse to support and finance terrorism was the highest. Nevertheless, the AT has the view that Slovakia has not specifically identified the types of NPOs which are vulnerable to FT abuse as required by the FATF standards.

26. The website of the MFA contains the links to relevant PF UNSCR (1718/2006 and 1737/2006, 1835/2008 and 2231/2015) which is considered by the REs as the main communication channel for PF TFS related issues. While the most material FIs in Slovakia are well-aware of their obligations on PF TFS, the exchange offices, non-bank payment institutions and most of the DNFBPs have a more limited understanding of TFS related obligations. They rely on manual, suspicious based checks performed against the lists published through the MFA's website.

Preventive measures (Chapter 5; IO.4; R.9–23)

27. The financial institutions have a good level of understanding of ML risks and are aware of their AML/CFT obligations, with the exception of payment institutions providing wire transfer services and exchange offices. The banking sector demonstrated a proactive approach to risks and good understanding of their AML/CFT obligations. The understanding of sector specific ML risks is less developed among DNFBPs (with some exceptions). Understanding of FT risks by most FIs and DNFBPs is confined to screening sanction lists, which include UN designation lists and lists of jurisdictions. Overall, there is a lack of comprehensive understanding of FT threats and vulnerabilities. Some DNFBPs (particularly dealers of precious stones and metals) had no knowledge of TF risk and respective obligations.

28. The internal controls and relevant risk mitigation factors are broadly understood by the FIs. All banks have sophisticated software tools to analyse risks and detect ML/FT indicators. The DNFBPs demonstrated insufficient knowledge about or availability of the key constituents of an ML/ TF risk mitigation framework.

29. The AT has some concerns regarding the depth of verification of BOs of legal entities. FIs met on-site stated that they do always identify natural persons behind the customer. However, the on-site interviews revealed certain gaps in the understanding of the concept of beneficial ownership.

30. In general, all FIs and DNFBPs could describe their suspicion reporting obligations. Some non-bank FIs and DNFBPs have not filed any UTRs nor identified any suspicions internally. Most UTRs are filed by banks for suspicions related to tax evasion, unknown origin of funds and *"virtual addresses"* of legal persons. Casinos demonstrated higher awareness of suspicious transaction indicators and frequently submitted UTRs, which mostly related to cases of criminal background of the client, unknown source of funds, card fraud, etc. FIs and almost all DNFBPs (except for real estate agents) demonstrated proper understanding on importance of tipping-off obligations.

31. All banks and larger FIs have appropriate control systems in place to mitigate ML/FT risks. Casinos and auditors appeared to have adequate internal policies and internal control procedures. Casinos reported that training is provided for staff periodically. Other DNFBPs (such as notaries, lawyers, real estate agents) do not have AML/CFT compliance structures in

place as the majority are sole practitioners. However, all of them had AML/CFT programs in compliance with the requirements of the AML/CFT Act.

Supervision (Chapter 6; IO.3; R.14, R.26–28, 34, 35)

32. The FIU and the NBS demonstrated a satisfactory level of understanding of the general ML/FT risks in their supervised sectors. There are weaknesses in the appreciation of specific ML/FT risks by the Gambling Regulatory Authority (GRA).

33. The NBS, the Gambling Regulatory Authority and the FIU are assigned responsibility for supervising AML/CFT compliance of FIs and casinos, respectively. In practice the NBS and the Gambling Regulatory Authority exercise their mandate for controlling compliance of supervised entities with all applicable AML/CFT requirements except the one on reporting to the FIU. In case the NBS identifies failure to submit an UTR, this information is provided to the FIU. The FIU also inspects the compliance with the AML/CFT requirements, including with the reporting obligations.

34. The scope and the depth of inspections conducted by the FIU and the NBS are not fully based on the AML/CFT risks. The reason behind is the lack of a documented process in place, which sets out how subject specific ML/FT risk-ratings drive frequency, scope and nature of future supervisory onsite/offsite inspections, as well as the lack of resources available for AML/CFT supervision. At the time of the onsite visit there was a lack of supervision in the MVTS sector. AML/CFT issues in the gambling sector have been covered to some extent during the holistic supervision conducted by the former supervisor (Ministry of Finance). As for the newly established Gambling Supervisory Authority (established in 2019), no AML/CFT inspections have been carried out yet.

35. The NBS established fitness and properness checks to prevent criminals and their associates from owning or controlling FIs, which seem adequate. However, it is not clear if in the on-going compliance monitoring with fit and proper requirements are always effective. Entry to the Casino sector is subject to a set of controls which include verification of criminal records on management and owners. Lawyers, notaries, tax advisors, accountants and auditors are subject to professional standards with adequate criminal checks. No checks are being conducted to prevent the criminals' associates from entering these sectors.

Transparency and beneficial ownership (Chapter 7; IO.5; R.24, 25)

36. Slovakia created the *"Register of legal entities, entrepreneurs and public authorities"* (hereafter the UBO register) in 2018. At the time of the on-site the Register was still being populated (only 12 % of legal persons inserted their UBO data into the UBO register) though the filling in of the register progressively continues. There are no mechanisms in place to verify the information on the UBOs at the time of registration. In the meantime, some control mechanisms are done ex post by state authorities, such as LEAs, tax authorities, as well as by media and NGOs.

37. The NRA analyses the ML/TF vulnerability of FIs and DNFBPs, as well as TF vulnerability of foundations, non-profit organizations and non-investment funds. However, this does not amount to a sufficiently comprehensive assessment of ML/TF risks stemming from the characteristics, nature and scope of activities of various types of legal persons that exist in the country. On a positive note, there is a clear understanding amongst all authorities that the limited liability companies are more likely of being misused for ML/TF purposes.

38. The LEAs, the FIU and the banks identified risks and took proactive mitigation measures in relation to *"virtual seats"* of legal persons and the use of *"straw men"* in corporate structures. The supervisors do not have sufficient understanding on this phenomenon.

39. Basic information on legal persons is contained in relevant registers. All competent authorities, including the supervisors, the LEAs and the FIU have direct access to all registers. The authorities considered the information contained therein to be accurate and up to date.

40. Information on the creation of all types of legal persons is publicly available.

International cooperation (Chapter 8; IO.2; R.36–40)

41. The SR has generally been active in providing constructive and timely MLA in relation to foreign requests, most of which were received and executed in direct cooperation with foreign counterparts. While the extradition regime has been performing satisfactorily, it is unclear whether domestic procedures were systematically initiated, upon the request of the respective foreign country, in cases where the extradition was refused on the basis of Slovakian citizenship.

42. The authorities were active in requesting MLA – although while every foreign elements of a criminal case must be supported by evidence obtained from abroad, there seems to be no practical mechanism to avoid requesting assistance from abroad (and thus to avoid the potential delays).

43. The FIU cooperates with its counterparts in a generally proactive and constructive manner, both spontaneously and upon request. As for the LEA these are equally engaged in frequent and constructive cooperation with their counterparts also at the operational level.

Priority Actions

1. Procedural and institutional measures should be taken to enhance and widen the use of financial intelligence. The financial aspect should be systematically explored by all LEA involved in detecting and investigating ML and proceeds generating crimes to: i) target ML and FT elements; ii) follow the trail of potential proceeds; and iii) identify other involved parties (such as beneficiaries of transactions). This is a fundamental building block of the AML/CFT mechanism which will enhance the entire repressive system. (IO7, 8, 9)

2. LEA should be provided with on-line access to various DBs and with tools to swiftly integrate the search results. A central bank account register for all legal and natural persons should be swiftly created and made available for the FIU and LEA. (IO6, 7, 9)

3. All LEA actors should be trained in the field of collecting and use of financial intelligence, and mechanisms to incentivise the police officers to better engage in financial analysis in ML and proceeds generating investigations should be adopted. (IO6)

4. The authorities should ensure that the FIU staff is properly motivated and have stable management. The FIU should substantially reconsider the dissemination system to ensure focus on the strong ML and FT suspicions, coupled with meaningful analysis to support the operational needs of LEA, in full respect of the confidentiality requirements. This action offers the opportunity to make a significant improvement quickly and at a relatively low cost for the country. (IO6)

5. Authorities should ensure that all registers have adequate resources and legal powers to hold accurate and up-to-date beneficial ownership information and effective, proportionate and dissuasive sanctions are applied against legal persons which do not comply with the requirement to submit relevant information. (IO5)

6. The supervisory authorities should allocate more resources and expertise to undertake

full risk-based supervision of FIs and DNFBPs. The NBS should consider having AML/CTF-dedicated supervisory staff. (IO3)

7. The Customs should enhance its understanding of ML/TF risks and obligations and develop sound mechanisms to be able to detect false or non-declarations and suspicions of either ML or FT (which could arise even where declarations are submitted). (IO6, 8)

8. The authorities should urgently review the legal and procedural framework for forfeiture/confiscation to identify the possible issues in the process and take appropriate steps to ensure that criminal proceeds are effectively confiscated in all cases. (IO8)

9. Extensive training should be provided to LEAs so as to enhance their knowledge of the possibilities provided by the existing legal framework for the confiscation and provisional measures (e.g. in the field of third-party seizure and confiscation). (IO8)

10. Slovakia should improve the legal and/or regulatory framework and appoint one state authority with clear responsibilities in order to increase the efficiency of the implementation of international sanctions. (IO10)

11. Slovakia should conduct the next iteration of the NRA which should be current, place an increased focus on serious threats and should comprehensively explore the full range of vulnerabilities. The NPO sector should be assessed according to the FATF requirements. (IO1)

Effectiveness & Technical Compliance Ratings

Effectiveness Ratings[3]

IO.1 – Risk, policy and coordination	**IO.2** – International cooperation	**IO.3** – Supervision	**IO.4** – Preventive measures	**IO.5** – Legal persons and arrangements	**IO.6** – Financial intelligence
Moderate	**Substantial**	**Moderate**	**Moderate**	**Moderate**	**Moderate**
IO.7 – ML investigation & prosecution	**IO.8** – Confiscation	**IO.9** – TF investigation & prosecution	**IO.10** – TF preventive measures & financial sanctions	**IO.11** – PF financial sanctions	
Moderate	**Low**	**Moderate**	**Moderate**	**Moderate**	

Technical Compliance Ratings[4]

R.1 - assessing risk & applying risk-based approach	**R.2 - national cooperation and coordination**	**R.3 - money laundering offence**	**R.4 - confiscation & provisional measures**	**R.5 - terrorist financing offence**	**R.6 - targeted financial sanctions – terrorism & terrorist financing**
PC	**C**	**LC**	**LC**	**LC**	**LC**
R.7- targeted financial sanctions - proliferation	**R.8 -non-profit organisations**	**R.9 – financial institution secrecy laws**	**R.10 – Customer due diligence**	**R.11 – Record keeping**	**R.12 – Politically exposed persons**
LC	**PC**	**LC**	**PC**	**LC**	**PC**
R.13 – Correspondent banking	**R.14 – Money or value transfer services**	**R.15 – New technologies**	**R.16 – Wire transfers**	**R.17 – Reliance on third parties**	**R.18 – Internal controls and foreign branches and subsidiaries**
PC	**LC**	**LC**	**LC**	**LC**	**PC**
R.19 – Higher-risk countries	**R.20 – Reporting of suspicious transactions**	**R.21 – Tipping-off and confidentiality**	**R.22 - DNFBPs: Customer due diligence**	**R.23 – DNFBPs: Other measures**	**R.24 – Transparency & BO of legal persons**
PC	**PC**	**LC**	**LC**	**PC**	**LC**
R.25 - Transparency & BO of legal arrangements	**R.26 – Regulation and supervision of financial institutions**	**R.27 – Powers of supervision**	**R.28 – Regulation and supervision of DNFBPs**	**R.29 – Financial intelligence units**	**R.30 – Responsibilities of law enforcement and investigative authorities**
LC	**PC**	**LC**	**PC**	**PC**	**PC**
R.31 – Powers of law enforcement and investigative authorities	**R.32 – Cash couriers**	**R.33 - Statistics**	**R.34 – Guidance and feedback**	**R.35 - Sanctions**	**R.36 – International instruments**
LC	**PC**	**PC**	**LC**	**PC**	**LC**
R.37 – Mutual legal assistance	**R.38 – Mutual legal assistance: freezing and confiscation**	**R.39 – Extradition**	**R.40 – Other forms of international cooperation**		
C	**LC**	**LC**	**LC**		

[3] Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.
[4] Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non-compliant.

MUTUAL EVALUATION REPORT

Preface

This report summarises the AML/CFT measures in place as at the date of the on-site visit. It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the AML/CFT system and recommends how the system could be strengthened.

This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 7-18 October 2019.

The evaluation was conducted by an AT consisting of:

- Ms Alina Andreea IONESCU – Legal Specialist, AML Unit, Financial Supervisory Authority, Romania (financial expert);
- Ms Zaruhi BADALYAN – Methodologist, Legal Advisor, Legal Compliance Division, Armenia (financial expert);
- Dr Lajos KORONA – Acting Head of Division, Metropolitan Prosecutor's Office, Hungary (legal expert);
- Mr Borislav ČVORO – Leading Investigator, Financial Intelligence Department – State Investigation & Protection Agency, Bosnia-Herzegovina (law enforcement expert);
- Mr Oleksandr HLUSHCHENKO – Director of Department for Financial Monitoring System Coordination State Financial Monitoring Service, Ukraine (law enforcement expert);
- Mr Vytautas KUKAITIS – Prosecutor of Public Prosecution Division, General Prosecutor's Office, Lithuania (legal expert)

MONEYVAL Secretariat:

- Ms Irina TALIANU – Administrator
- Ms Astghik KARAMANUKYAN – Administrator
- Mr Alexey SAMARIN – Administrator

The report was reviewed by FATF Secretariat, Ms Adriana Ion, FIU (Romania), Ms Jana Ružarovská, FIU (Czech Republic).

The Slovak Republic previously underwent a MONEYVAL Mutual Evaluation in 2011, conducted according to the 2004 FATF Methodology and was placed under regular follow-up procedure.

That previous MER concluded that the country was compliant with 5 Recommendations; largely compliant with 18; partially compliant with 23; non-compliant with 2; and not applicable with 1. The Slovak Republic was rated compliant or largely compliant with 7 of the 16 Core and Key Recommendations.

CHAPTER 1. ML/TF RISKS AND CONTEXT

1. The Slovak Republic is a parliamentary republic located in Central Europe, bordered by Ukraine and four other EU countries: Poland, Hungary, Austria and the Czech Republic. It has a population of 5 447 011 and a GDP of USD106 472 Billion (World Bank estimate, 2018). The capital city is Bratislava. Its official currency is the Euro (EUR).

2. According to the 2017 census, the majority of inhabitants are Slovaks (81.45%) and the Hungarians are the largest ethnic minority (8.33%). Other ethnic groups include Roma (2,04%) and Czechs, Moravians and Silesians (0.6%)[5].

3. The largest share of the Slovak economy is accounted for by the tertiary sector, contributing around 56% to GDP, in which about 61% of the working population find employment. The industrial sector also plays a significant role within its economy, contributing to 31% of GDP. The main industry sectors are car manufacturing and electrical engineering. Exports and foreign direct investments are increasingly important for the entire Slovak economy. The average monthly earning *per capita* 2019 is of EUR 1 064.

4. Slovakia is a member of the European Union and of other international organisations such as the Council of Europe (CoE), the Organisation for Security and Cooperation in Europe (OSCE), the Organisation for Economic Co-operation and Development (OECD), the North Atlantic Treaty Organization (NATO), the UN, the World Trade Organisation (WTO), as well as the regional group Visegrád Four (V4: Slovakia, Hungary, Czech Republic and Poland).

1.1 ML/TF Risks and Scoping of Higher-Risk Issues

Overview of ML/TF Risks

5. This section of the mutual evaluation report presents a summary of the AT's understanding of the ML/TF risks in Slovakia. Slovakia's assessment and understanding of the risk is set out in "Country's risk assessment" and in Chapter 2.

6. This summary is based on Slovakian NRA, open source material, as well as discussions with competent authorities and the private sector during the on-site visit. As further detailed in the sub-chapter below, the AT considers the NRA has a series of weaknesses which limited the accurate understanding ML/TF threats.

7. There is a reported decrease in overall reported crimes, with a consequent decrease in the value of the total damage caused by criminality. According to the NRA statistics, the offences generating the highest damage are frauds in various forms (credit, tax), theft, embezzlement, tax and insurance evasion, and failure to pay tax and insurance.

8. Domestic reports have limited information on the range of criminal activities carried-out by organised crime groups (OGC) active in Slovakia. Nevertheless, the threat posed by the drug production and trafficking must be considered, as the EUROPOL SOCTA Report lists Slovakia as one of the main producers of Methamphetamine in the EU[6]. The same Report refers to Slovakia in the context of links with Italian mafia clans in a case of firearms trafficking[7].

9. Corruption remains an area for concern and an important source of illicit gains in Slovakia. There were few noticeable corruption related investigations or convictions (recently two former

[5] Statistical Yearbook of the Slovak Republic 2018.
[6] Europol, "EUROPEAN UNION Serious and organised crime threat assessment 2017" – page 39
[7] IDEM –page 54

Ministers have been convicted for corruption crimes committed in 2006-2010). In February 2018 an investigative journalist[8] - known for his reporting on fraud cases and tax evasion related to high-profile politicians and businessmen - and his fiancé were killed. Media reports containing allegations of collusion between OCG and Slovak politicians and LEA abounded after the murder.

10. The conclusions of a recent GRECO report[9] confirms the lack of mitigation measures taken in relation to the corruption threat at top executive functions level, and highlights that there is an immediate need for an operational plan to combat corruption within the police.

11. Slovakia does not have specific data available to estimate the country's exposure to cross-border illicit flows (related to crimes in other countries). There is little information on the techniques used or the degree to which foreign proceeds are being laundered in Slovakia. Discussions with investigative authorities and the FIU did not provide a great deal of information regarding the source, nature and scope of the threat from cross border illicit flows beyond the stolen cars trafficking.

12. The authorities do not consider significant the risks related to cash and BNI being smuggled through Slovakia. Nevertheless, due to its geographical situation in Central Europe and the free movement of persons, goods and services within the Schengen area, Slovakia may be misused for cross-border crimes and the development of trade routes in illicit flows of goods and funds.

13. In 2018, one arrest for terrorism-related offences in Slovakia has been registered[10]. There are no signals of a terrorism threat coming from domestic, regional or global sources. The AT could not identify any indication that the terrorist or TF threat could be other than *"medium-low"* as defined by the NRA particularly since in the three on-going TF investigations, a decision has not yet been pronounced by the Slovak Courts.

14. The main vulnerability of the country resides in the limited ability of the authorities to search, seize and confiscate illegally acquired property to deter crime. The sectoral ML vulnerability is born by the banking sector due to its size and weight in the overall financial sector.

Country's risk assessment

15. The first Slovak anti-money laundering (AML), countering terrorism financing (CTF) NRA was finalised in 2017, publicised in 2018 and formally adopted by the Government in 2019, using statistics and other data collected for the period 2011-2015. There is a significant time gap between the data analysed and the moment of the adoption of the report which makes the results of the analysis questionable in terms of actual relevance in the now-days ML/FT dynamic context. As the reader can see in the above sub-chapter, the AT does not consider the findings of the NRA fully comprehensive.

16. Under the coordination of the FIU, a team of almost 70 members from all relevant authorities (e.g. Ministries of Finance, Justice, Defence; GPO; National Bank; SIS; Police) and the private sector (e.g. professional associations and chambers) cooperated in the establishment of the assessment.

17. The NRA was done the World Bank methodology and it is structured in three parts: i) ML risk (which contains separate *"Threat"* and *"Vulnerabilities"* chapters); ii) ML vulnerabilities in particular economic sectors and iii) TF risks.

18. The NRA contains a non-public version, which was not available to the private sector. The

[8] Mr Jan Kuciak
[9] https://rm.coe.int/grecoeval5rep-2018-9-final-eng-slovakrep-public/168096d061
[10] European Union Terrorism Situation and Trend Report 2019 (Europol)

authorities have different views on the utility if the non-public section: some consider it of significance for the threat assessment while others see it more as a particularization of already existing conclusions.

19. The level of the national ML risk was determined based on an assessment of a) the level of threats of the legalisation of proceeds of crime at national level, and b) the level of vulnerability in relation to the legalisation of proceeds of crime at national level. This entailed both an assessment of qualitative and quantitative information on the nature of income and proceeds derived from criminal activity or financing, and an assessment of the shortcomings and weaknesses of Slovakia's AML framework. The level of the national TF risk was established as a result of an assessment of the national terrorist threat; an evaluation of the direction, resources and channels which were usable for TF purposes; and an assessment of the strengths and weaknesses of the CTF-framework.

20. Relevant sources of data were: activity reports of competent authorities, regular and *ad-hoc* evaluation and analytical reports, typological studies, Slovakia's assessments prepared by international organisations, and statistical data obtained through questionnaires. The Working Group also analysed relevant primary and secondary legislation and held discussions with relevant entities. A grand difficulty experienced when drafting the NRA was the lack of comprehensive data and statistical indicators.

21. The NRA estimates the overall level of the ML threats in Slovakia as *"medium"* with an increasing trend. The following ML threats have been identified: a) criminal offenses against property (theft), b) criminal offenses of economic nature (tax crimes, fraud, damage to the financial interests of the European Communities), and what is was labelled in the NRA as *"Specific partial types of crime"*, including corruption, drug-related crime and organized form criminality and cybercrime. Corruption is seen as *"medium-high"* threat in Slovakia but is only marginally examined in the public version of the NRA (to which the private sector had access to). A more granular analysis is available in the non-public part of the NRA which still lacks typologies and corruption related ML trends and features.

22. Is the AT's view that the *"Vulnerabilities"* chapter is the soundest part of the NRA. It points to the authorities' ability to fight ML, including insufficient staffing and financial resources of the financial intelligence unit (FIU) and the supervisors. The lack of specialization in identifying and tracing of proceeds and in performing financial investigations which results in insufficient seizure and confiscation of proceeds of crime is also identified as a deficiency. Other, more detailed shortcomings have been identified such as absence of a central bank account register; inefficient data management systems and statistical data, and lack of systematic training of law enforcement agencies (LEAs) and courts in the area of ML and proceeds recovery.

23. Turning to ML techniques, the NRA concludes that after thoroughly analysing the practices and activities ML perpetrators used to hide the illegal income and proceeds, the Working Group identified the most used forms and methods of legalization: i) the majority of the proceeds are subject to immediate consumption by the perpetrator of the predicate offense, without specific elements of the legalization moment; transfers to foreign bank accounts 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.

24. While accepting that the above finding is in line with the NRA, as stated above, the AT has reservations on the accuracy of this conclusion as a cascading effect from the limited nature of the *"Threats"* identified, which do not fully consider more serious and sophisticated forms of criminality.

25. At sectoral level, the most vulnerable is the banking sector, although the conclusion needs

more substantiation. The particular vulnerabilities identified are basically a full list of (potential) supervisory and preventive measures failures[11] rather than a meaningful analysis of actual weaknesses based on a country-specific analysis.

26. The overall level of the TF threats in Slovakia was rated "low" in the NRA. The conclusion is mostly based on the absence of terrorist acts in Slovakia and in the neighbouring countries as well as the geographical position which minimizes the threat of cross-border cash transfers for TF purposes. The overall TF risk is considered as *"medium-low"*. While not challenging the actual risk level, the AT found that the NRA lack granularity and includes a listing of rather general TF related risk than a sound analysis of trends, sources, financial products and services that could be misused. Some terms are used interchangeably as for instance the *"ineffectiveness of financial intelligence/intelligence"* is listed as a threat, while the AT's opinion this constitutes vulnerability. The analysis of risks into categories (collection, movement, usage) is absent.

27. According to information provided, a limited number of NPOs is vulnerable to TF. The NRA states that in the period under review, between 2011 and 2015, there were no cases where NPOs were used or misused for ML or TF.

Scoping of Higher Risk Issues

28. In deciding what issues to prioritise for increased focus, the assessors reviewed the Slovakian NRA, and information from third-party sources (e.g. reports of other international organisations). The assessors focused on the following priority issues:

- **Corruption:** Transparency International (TI) corruption perception index ranks the Slovak Republic on 57th place out of 180 countries, what is a drop of three positions compared with 2017. The AT considered whether the risks associated with corruption have been properly assessed, and whether combating measures are equal. Moreover, the assessors focused on potential impact of corruption on the competent authorities responsible for the AML/CFT both on preventive and repressive measure.
- **Tax and Insurance evasion, tax fraud.** The NRA ranks tax-related predicate offences as high-risk ML threats and described as crimes that generate the highest damage to the economy of the country and have a significant potential and increasing trend. The assessors focused on the actions taken by the competent authorities regarding tax crimes and related proceeds and effectiveness of these measures.
- **Organized crime (OC).** The organized form of crime is a permanent ML threat in Slovakia. According to the information from the authorities, smuggling or illegal supplies of high-tax goods, trafficking in human beings become more intensive and increase illegal income of OC groups. The NRA mentions smuggling of migrants as another source of proceeds likely to be laundered. The journalists' murder case raises questions of possible interference of Slovak mafia into LEA work.
- **Asset recovery:** In Slovakia the preparation of law enforcement authorities, including courts, in conviction-related matters of ML/TF cases appears rather weak. There is not one specialized entity managing all the seized assets (and the execution of property-related decisions) in a comprehensive manner. The results in confiscation of proceeds and income of criminal activity (and, consequently, the asset recovery) also appears low.

[11] *i.a.* (low) effectiveness of supervisory practices and methods; enforcement of administrative sanctions; awareness on AML measures by all banks employees; effectiveness of the bank responsible for compliance (sic!); effectiveness of UTR monitoring and reporting; availability and access to BO information.

- **Gambling sector.** The NRA indicates the gambling industry as a target for OC investments and subsequent laundering purposes. This raise concerns not only to the application of AML/CFT preventive measures by the sector, but also on the authorities' ability to properly *"fit and proper"* test the ownership of the gambling operators. The evaluation team also focused on the activities of the Gambling Regulatory Authority, which took the responsibility of supervising casinos in June 2019.
- **Banking sector.** The total assets of FIs that operate in the sector have a 90% share of GDP in the Slovak Republic. Of these, there are three major banks that dominate the sector and account for over 50% of its total assets. According to the NRA, the banking sector carries a "medium-*high"* level of ML threat and the same level of vulnerability. The AT focused on CDD measures applied by banks in respect of clients.
- **Supervisory arrangements and practice.** The AT considered the risks and vulnerabilities stemming from the current level of resources allocated to the supervision of financial institutions (FIs) and designated nonfinancial businesses and professions (DNFBPs). Considerable attention was also paid to the division of responsibilities between the FIU and sectoral supervisors (the NBS and the Gambling Regulatory Authority) for supervising AML/CFT compliance of FIs and DNFBPs. The AT also focused on the supervisory authorities' understanding of sector's risks, effectiveness of supervisory procedures and the reporting system.
- **Transparency of legal persons.** The authorities have identified recently risks with regard to *"virtual seats"* of legal persons and the use of *"straw men"* in corporate structures. The assessors analysed the effectiveness of the country's mechanisms aimed at ensuring the transparency of these entities.

1.2 Materiality and level of ML/TF risks of the different FIs and DNFBPs

29. The Slovak economy is small but knows a strong financial system (without being a financial centre), dominated by foreign groups. It has shown a positive economic trend over the last number of years. The OECD estimates that the economy will continue to grow and even show the highest GDP growth rate among OECD economies. The European Commission's country report on Slovakia (2019) noted the high economic growth and low unemployment rate, while also pointing critically towards the regional imbalances and the weak performance of the public sector, education, science and research.

30. The tertiary, services sector, dominated by trade and real estate, contributes to 55.94% of GDP and employs around 60.8% of the workforce. The secondary, industrial sector is the second important contributor to economy, employing 36,07% of the workforce and representing 30.97% of GDP. Slovakian economy relies on industry and manufacturing and on the exportation of goods and services, mainly in the automotive sector and consumer electronics[12]. Lastly, the agriculture sector is little developed, represents only 3.3% of GDP and contributing to 2.8% of employment of the working population in 2018.[13]

31. The banking sector accounts for more than 70% of total financial sector assets in 2018; insurances (7.14%) and investment funds (7.13%) come next.[14] As of 2018, there are 12 Slovak and 15 non-Slovak (EU) banks registered, as well as 14 Slovak and 21 non-Slovak (EU) insurance

[12] https://databank.worldbank.org/views/reports/reportwidget.aspx?Report_Name=CountryProfile&Id=b450fd57&tbar=y&dd=y&inf=n&zm=n&country=SVK

[13] World Bank data, via https://en.portal.santandertrade.com/analyse-markets/slovakia/economic-outline

[14] Annual report of the NBS, 2018

companies registered together with 40 securities companies. From the 12 Slovak banks, 8 have foreign ownership worth more than 50% and the remaining 4 banks have 100% resident shareholders. The value of assets maintained in the latter 4 banks is almost 6 times higher than for the 8 foreign ownership banks. All of the above implies that the banking sector is the most material in the country.

32. The size of the informal economy in 2014 was set by Eurostat on 14.6% of GDP.[15] The Slovak experts estimated this number to be higher, which indicates the perception that the informal economy remains a significant concern.

33. The assessors classified obliged sectors on the basis of their relative importance, given their respective materiality and level of ML/FT risks. The assessors used this classification to inform their conclusions throughout this report, weighting positive and negative implementation issues more heavily for important sectors than for less important sectors. This approach applies throughout the report but is most evident in IO.3 and IO.4:

a) most significant: the banking sector based on the overall market share, as well as known ML/FT cases;

b) significant: gambling sector and securities providers based on exposure to ML/FT risks; MVTS due to lack of identification of all service providers and ML/TF typologies identified;

c) less significant: other FIs, including insurance, and other DNFBPs.

1.3 Structural Elements

34. The key structural elements which are necessary for an effective AML/CFT regime are present in Slovakia. It has democratic institutions in place, including rule of law and human rights guarantees. The level of democracy is rather high, scoring 2.61 out of 7 (with 1 being most democratic and 7 least democratic) in 2017.[16]

35. Justice in Slovakia is administered by the ordinary law courts and the Constitutional Court of the Slovak Republic. The judicial power is exercised by independent and impartial courts. At all levels, judicial matters are separated from those of other national authorities.

1.4 Background and other Contextual Factors

36. In 2018 Slovakia scored 50 points out of 100 on the 2018 Corruption Perceptions Index reported by TI and ranks 57 out of 180.

Table 1: Corruption Perception Index between 2015 and 2018

Year	CPI (0 = high, 100 = low corruption level)	Rank (out of 180)
2015	51	50
2016	51	54
2017	50	54
2018	50	57

37. Besides corruption, tax evasion remains a serious challenge for Slovakia. Although taxes on production and imports (*e.g.* VAT) as a share of GDP are below the EU average (the tax-to-GDP ratio in Slovakia is 33.% of GDP), for Slovakia it is the second largest source of revenues.[17] The

[15] https://www.eurofound.europa.eu/publications/article/2017/slovakia-combating-undeclared-work-views-and-experiences-of-the-actors-involved

[16] https://freedomhouse.org/report/nations-transit/2018/slovakia

[17] Eurostat, 2017.

authorities are aware of the situation and several measures have been taken to limit the evasion and to improving tax collection. As part of the Action Plan to Combat Tax Fraud, between 2012 and 2017 the Government has implemented 50 measures. The most important include the VAT control statement and the mandatory VAT advance on registration for high-risk applicants. The Slovak Government approved the proposal of the Action Plan to Fight against Tax Evasion for the period 2017 – 2018, which contains 21 new actions aimed to eliminate new forms of tax frauds (*i.e.* a specific measure which combine administrative and enforcement measures called TAX COBRA).

38. The level of financial inclusion is relatively high in Slovakia, as it is estimated that 84% of adults have an account.[18] The use of cash is identified as a risk factor for ML/TF.

AML/CFT strategy

39. Slovakia has developed an AML/CFT 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. The Strategic Plan was informed by the MONEYVAL Fourth Round MER. It focused particularly on the deficiencies relating to criminal investigations, as most LEAs merely documented predicative crimes and did not deal with the subsequent legalisation of their proceeds.

40. Following from the outcomes of the NRA and the subsequent AP, new Strategic Principles to Combat Money laundering and Terrorist Financing for 2019-2024 have been adopted. They give extra consideration to the private sector, in particular to the comprehensive and correct application of the obligations in the prevention and detection of possible forms of legalization and terrorist financing; mutual cooperation and exchange of information between the public sector and the private sector; and to the education and training system in this field.

41. The Action Plan to Combat Legalization of Proceeds of Criminal Activity, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction 2019 – 2022 was adopted by Government Resolution on 7 May 2019 and contains a series of "Orders" and "Recommendations" for the most important players in the AML/CFT area, such as the MoI, the MoJ, the MoF, the NBS, the Police, the GPO, the FIU.

Legal framework

42. Most notably within the AML/CFT legal and organisational framework is the 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 (hereafter the AML/CFT Act), which has been amended a number of times since its adoption. The AML/CFT Act establishes the rights and obligations of legal persons and natural persons in the prevention and detection of legalization of proceeds of crime (hereinafter: the "legalization") and terrorist financing and establishes the competent authorities and their responsibilities within the AML/CFT framework. The European Union's 4th AML Directive has been transposed into this Act.

43. Other relevant legislation includes the Criminal Code (hereafter CC) and the Code of Criminal Procedure (hereafter CCP), Act no. 289/2016 on the Implementation of International Sanctions (ISA), Act No. 566/1992 on the National Bank of Slovakia, Act No. 747/2004 on Financial Market Supervision, Act No. 483/2001 on Banks, Act No. 199/2004 on Customs and Act 46/1993 on the Slovak Information Service (SIS).

[18] https://microdata.worldbank.org/index.php/catalog/3270/download/44216

Institutional framework

44. The following are the main ministries and authorities responsible for formulating and implementing the government's AML/CFT and proliferation financing policies:

45. **The Financial Intelligence Unit of the Presidium of the Police Force (FIU):** According to art. Art. 26 (1) of the AML/CFT Act, the FIU shall serve as a national unit for the area of the prevention and detection of legalization and terrorist financing. Since the last evaluation, the FIU was subject to structural changes inside the Police organizational and is now under the direct supervision of the President of the Police force.

46. **National Criminal Agency (NAKA)** is an organizational unit of the Police Force Presidium. Its competence is regulated by the Regulation of the Minister of Interior of the Slovak Republic No. 175/2010 (art. 5). As the successor of the previously independent anti-corruption and organised crime authorities of the Presidium of the Police Force, NAKA was established with the aim to increase the effectiveness of official activities in the field of combating crime. It was also needed to unify the activities of the various offices working on serious crime to prevent duplication of operational activities and criminal proceedings. Within the structure of NAKA, the following executive units have been set up (until Oct 2019):

- Financial Police Unit NAKA,
- Anti-Crime Unit NAKA,
- Anti-Drug Unit NAKA,
- Counter-Terrorism Unit NAKA,
- Property Investigation Department NAKA

47. **Police Force units** 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 NAKA. 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.

48. **General Prosecutor's Office (GPO)**: the General Prosecutor's Office is the central state authority and the supreme body of the Public Prosecution, headed by the Prosecutor General, and divided into various units. The Public Prosecution is constitutionally constituted as an independent *sui generis* public authority. The Public Prosecutor's Office is composed of the GPO, the 8 regional prosecution offices and the 54 district prosecution offices. The execution of prosecution activities in the area of prosecution of money laundering is carried out by prosecutors of the criminal department of individual organizational units of the prosecution office.

49. **The Special Prosecutor's Office (USP)** has the national 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. It is part of the GPO. The execution of prosecution activities in the area of prosecution of terrorist financing is solely carried out by the prosecutors of the Office of Special Prosecution.

50. **The Ministry of Justice (MoJ)** prepares and submits legislation in the areas of *i.e.* constitutional, criminal and civil law, as well as status laws for *i.e.* lawyers, notaries and enforcement officers and laws related to the exercise of judicial powers and the activities of the prosecutor's office. It provides, coordinates and/or provides assistance to courts in the field of judicial cooperation (in criminal, civil and business matters). It also supervises the activity of courts, performs state supervision of the activities of the Slovak Chamber of Executors and the

Chamber of Notaries of the Slovak Republic, and to the statutory extent over the activities of notaries and enforcement officers. It administers the Collection of Laws, the Commercial Register and the Register of Public Sector Partners.

51. **The Ministry of Finance (MoF)** is responsible for creating legislation related to finance, taxes and fees, customs, financial control, internal audit and government audit, as well as budgeting of the general government deficit, budget development and implementation, financial market policy development and implementation, and policy for management of public assets in the welfare (public benefit) and non-business sector.

52. **The Financial Administration Criminal Office (FACO) –** is the special LEA type body responsible for detection and investigation of criminal offences related to tax, added value tax, excise duties or custom regulations, including associated ML.

53. **The Ministry of Interior (MoI)** is the main guarantor of the fight against terrorism and organized crime in Slovakia, organizes the FIU and coordinates the Police.

54. **Slovak Information Service (SIS)** has responsibilities in the area of combating organised crime and terrorism, including in the ML/TF area. It also performs tasks under specific laws in the fight against the proliferation of weapons of mass destruction (WMDs). It acquires, collects, evaluates and verifies information and signals about the activities of persons or organizations that are related to or may be related to terrorist acts.

55. **Military Intelligence (MI)** has responsibilities in the area of combating terrorism, including in the ML/TF area. It performs these tasks under specific laws. It acquires, collects, evaluates and verifies information and signals about the activities of persons or organizations that are related to or may be related to terrorist acts.

56. **National Bank of Slovakia (NBS)** provides supervision in the AML/CFT area in accordance with the Act No. 747/2004 (on Financial Market Supervision) and the AML/CFT Act. It lays down prudential business rules; monitors compliance with the provisions of the Acts and other special laws and regulations, it issues authorisations, licences, prior consents, imposes sanctions and imposes remedial measures; and it conduct on-site inspections and off-site supervision of financial market entities.

57. **Customs Administration** is responsible for detection, monitoring and reporting of cross-border cash transactions. It controls the fulfilment of the obligation to file a cash transaction reports which are provided to the FIU**.**

Financial sector and Designated Non-Financial Businesses and Professions (DNFBPs)

Financial institutions

58. The banking system plays an important role in the entire economy of Slovakia, although the banking sector is one of the smallest in the EU in comparison to the national GDP.

Table 2: Financial Institutions in Slovakia (2018)

Financial Institutions		
Sector	**No. of Registered Institutions**	**Value of assets (in EUR)**
Banks	27	EUR69 544 067 000 EUR10 463 396 000
Insurance companies	35	EUR7 239 027 698 EUR1 187 983 589
Insurance agents	23 007	n/a
Payment institutions	9	EUR88 543 376
Agents of Foreign payment institutions from	6 (37 agents)	n/a

EU member countries		
E-money institutions	1	EUR3 368 513
Securities companies	41	EUR402 165 000
Assets management companies	8	EUR8 338 763 000
Currency exchange operators	1 167	n/a
Pawnshops	20 994	n/a
Lenders	31	EUR4 391 241 670
Credit intermediaries other than banks and savings banks[19]	12,134	n/a
Investment pension funds[20]	6 (Pension Fund Management) 4 (Supplementary Pension Fund Management)	EUR8 059 867 000 EUR2 009 084 000
Leasing companies	33 000	N/A
Auctions	711	N/A
Trader with claims	**39.860**	N/A

Table 3: Ownership structure of commercial banks

Ownership structure of commercial banks in 2018		
	Number	**Value of assets**
Foreign ownership more than 50%	8	EUR9 106 828 000
Foreign ownership less than 50%	0	0
Resident Shareholders 100%	4	EUR60 437 239 000
Foreign Branches	15	EUR10 463 396 000
Total number of banks	27	EUR80 007 463 000

59. The Slovakian banking sector consists of 27 financial institutions with banking licences. Most of them are universal banks, focused on retail and corporate banking. Four of them are specialised banking institutions (three building societies and a state-owned development bank). Since privatisation ended in 2001, most of the banks in Slovakia are controlled by foreign entities, mainly banking groups from Austria, Italy and Belgium. Only four banks are fully controlled by domestic investment groups (three banks) or government (one bank). The Slovakian banking sector is concentrated within the hands of three major players who control more than 50% of the banking assets. Despite this concentration, the market share of small and medium-sized banks has slightly increased in recent years[21].

60. Slovak banks are among the leaders in the use of new technologies in day-to-day banking *e.g.* contactless cards, contactless mobile payments and peer-to-peer payments[22].

61. The following entities operate in the Slovak insurance market:13 insurance companies based in the SR; 22 insurance companies based in another EU State through a branch; and 650 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 is

[19] Independent Financial Agent (FA): 216; Subordinate FA: 8,936; Tied FA: 2,982

[20] The Pension fund products (Pillar III, Pillar II) are offered by an independent financial agent.

[21] European Banking Federation https://www.ebf.eu/slovakia/

[22] European Banking Federation https://www.ebf.eu/slovakia/

approximately 7,4%.

62. Foreign exchange activity is carried out by banks and branches of foreign banks, and exchange offices based on the foreign exchange license issued by the NBS.

63. The payment services provide products based on cash or international cashless transfers and include the following activities: crediting and debiting a payment account with cash and all other operations required for the operation of a payment account; carrying out payment operations, including money transfers; carrying out payment operations when the funds are covered by a credit line for a user of payment services; issuing and/or accepting payment cards and other payment instruments; money remittance; and payment operations when the payer's consent is expressed through any electronic, digital or information communication devices.

DNFBPs

64. The competent authorities do not have the exact number of obliged entities in this area: businesses have in many cases several licenses based on which they can be considered an obliged entity, but some do not use licenses at all.

65. 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 FIU. It is also a vulnerable place in terms of both AML/CTF control and general supervision.

Table 4: Number of DNFBPs in Slovakia (2018):

Type of business	No. of Registered Institutions
Gambling operators	182
Legal p. or natural p. authorized to mediate sale, rent or purchase of real estate	100 934
Traders in precious metals or gemstones	4 749
Pawnshops	20 994
Auditors	1 022
Tax advisors	953
Accountants	450 890
Lawyers	5 840
Notaries	340
Bailiffs	281
Service provider for trade companies	N/A
Postal undertaking	27
Administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings	765
Legal or natural persons acting as economic advisor	1 102 149

66. The following categories of the non-financial sector are the largest: accountants; pawnshops; organisational and economic advisors; lawyers; and real estate mediators.

Preventive measures

67. The primary piece of Slovakian legislation covering preventive measures in the AML/CFT framework (including customer due diligence, reporting, and record-keeping) is the AML/CFT Act (no. 297/2008 Coll.), which includes also terrorist financing issues. The preventive measures regime applies to both financial institutions and DNFBPs. In addition to the AML/CFT Act, the FIU, supervisory authorities and other competent authorities have issued sectorial regulatory acts. All categories of FIs and DNFBPs as required by the FATF Standards are covered by the preventive measures.

Legal persons and arrangements

68. All Slovakia's legal entities are registered in the Commercial Register. Entrepreneurial activity can be performed under the following legal forms: individual entrepreneurs; limited partnerships; unlimited partnerships; joint-stock companies; simple joint stock companies; limited liability companies; co-operatives; state enterprises; associations, non-profit organizations, non-investment funds, foundations and cooperatives.

Table 5: Types of legal persons and arrangements (as of 31 December 2018)

Type of Legal Persons / Arrangements	No. Registered (where available)
Foundation23	1 454
Non-investment fund* **	584
Non-profit organization providing generally useful services* **	3 250
Cooperatives:	2 541
Limited liability company	262 218
Joint-stock company	7 367
Limited/unlimited partnership company	2 420
Public trade company	943
Simple joint stock companies	119

69. The legal system of Slovakia does not regulate the trusts. Under the AML/CFT Act, trusts have no exceptions in the assessment of transactions, in the identification of the BO, or in the performance of CDD or EDD.

70. The AML/CTF system of measures and responsibilities at the national level also applies to NPOs in addition to obliged entities. Under Art. 9(e) AML/CFT Act, NPOs are defined as corporations, which are understood as foundations, non-profit organizations providing generally useful services, non-investment funds and other special-purpose corporations irrespective of their legal personality which manage and distribute funds. The largest organisations in the NPO sector in terms of financial volume are foundations. NPOs are obliged to identify the donor and identify the natural person or legal entity to whom the NPOs have provided funds if the donation value or

[23] Act No. 52/2018 Coll. amended the AML Act No. 297/2008 Coll. where in Article 25 par. 1, obligations were defined for corporations (see the table above) for the identification of the donor and identification of the natural or legal person whose corporation has provided funding if the value of the donation or the amount of funds provided reaches at least EUR 1 000. Under Article 25 par. 2, the FIU is authorized to carry out an inspection pursuant to Article 29 in corporations for the purpose of identifying the beneficial owner and verifying the truthfulness and completeness of the data on the beneficial owners, identification of persons under par. 1 or for the purpose of checking the disposal of the property. During the inspection, the corporation has the same obligations as obliged entities under Article 30. According to the AML Act, corporations are regulated in Article 9 e), under which a corporation means a foundation, non-profit organization providing generally useful services, non-investment fund or another special-purpose corporation irrespective of its legal personality which manages and distributes funds.

the amount of funds provided reaches at least EUR 1 000. The NPOs shall be registered in the Register of Non-Governmental Non-Profit Organisations (functionable as of 1 January 2021), which will be administered by the Ministry of Interior.

Supervisory arrangements

71. The AML/CFT supervision framework is consolidated mainly under the NBS and FIU. For financial institutions the NBS is the main licencing and supervisory authority, including for AML/CFT and purposes. At the same time the FIU is also designated as the AML/CFT supervisor for FIs:

Table 6: Supervisory arrangements financial institutions

Financial Institutions	
Sector	**AML/CFT Supervisor**
Banks	FIU/NBS
Insurance companies	FIU/NBS
Insurance agents	FIU/NBS
Payment institutions	FIU/NBS
Agents of Foreign payment institutions from EU member countries	FIU/NBS
E-money institutions	FIU/NBS
Securities companies	FIU/NBS
Assets management companies	FIU/NBS
Currency exchange operators	FIU/NBS
Pawnshops	FIU
Lenders	FIU/NBS
Credit intermediaries other than banks and savings banks[24]	FIU/NBS
Investment pension funds[25]	FIU/NBS
Leasing companies	FIU
Auctions	FIU
Trader with claims	FIU

Table 7: Supervisory arrangements DNFBPs

Type of business	**AML/CFT supervisor**
Gambling operators	FIU, MoF
Legal p. or natural p. authorized to mediate sale, rent or purchase of real estate	FIU
Traders in precious metals or gemstones	FIU
Pawnshops	FIU
Auditors	FIU
Tax advisors	FIU
Accountants	FIU
Lawyers	FIU
Notaries	FIU

[24] https://www.nbs.sk/en/financial-market-supervision1

[25] A bank; the Central Securities Depository; a Stock Exchange

Bailiffs	FIU
Service provider for trade companies	FIU
Postal undertaking	FIU
Administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings	FIU
Legal or natural persons acting as economic advisor	FIU

International Co-operation

72. Slovakia is engaging in a variety of international initiatives in the area of AML/CFT. It is a member of MONEYVAL and the Egmont Group of FIUs, and it participates in international meetings of the Council of Europe, the Conference of the Parties of the Warsaw Convention (on AML/CFT, MLA and international co-operation), FATF, UNODC, OSCE, World Bank and other international organisations, agreements are in place with NATO, among others. International cooperation is carried out based on non-contractual reciprocity and on the basis of international treaties of which the provisions are directly binding in Slovakia.

73. The performance of international cooperation on the exchange of financial intelligence and other relevant information and data to combat ML and TF is done by the FIU. The NBS cooperates in the supervision of the financial market and exchanges information to the extent necessary for the performance of its tasks and under the conditions laid down by the Financial Market Supervision Act and special regulations. The SIS and MoI are authorised to cooperate with authorities of other countries of similar specialisation and scope in the performance of its tasks. LEAs cooperate with foreign partners under the Police Force Act. Prosecutors have to apply the provisions of the international treaties and Slovak laws. The Order of the Prosecutor General of the Slovak Republic (from 13 December 2016) provides further guidance on the actions of the prosecutors in the field of international cooperation in criminal matters.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

2.1. Key Findings and Recommended Actions

Key Findings

1. Most of the authorities' understanding of risk is limited to the NRA therefore, its' shortcomings negatively impact the mitigation measures undertaken. The results of the NRA are considered by the NBS and the FIU when performing supervisory activities. Prosecutors appear to have a more accurate and comprehensive understanding of ML threats including organised crime, corruption in the broad sense, and cybercrimes.

2. The AT has some concerns about the accuracy of the NRA's findings which impacts on the country's understanding of ML/TF risks given that: certain risks (including the use of fictitious companies, the Fintech sector, the use of cash and external threats), have not received a significant attention; the NRA does not provide a comprehensive description of the main ML methods, trends and typologies and the time lag. The assessment of TF risks is an area for improvement. The AT deplores the length of the NRA adoption procedure and the time gap between the data-source and the outcome.

3. The Slovak Republic has established a good foundation for an effective national coordination and cooperation to address ML/TF risk both at policy and operational levels. The Interdepartmental Expert Coordination Body on Combating Crime (MEKO), the Council of the Government for Criminality Prevention and the Multidisciplinary integrated group of experts on ML and TF and PF (NES-LP), occupy an essential place in the national coordination system. Nevertheless, a more substantial high-level commitment in the area of combatting ML and TF at the policy level is still needed.

4. To some extent, Slovakia's national AML/CFT policies aim to address the identified ML/TF risks. Although its policies and plans can be general and dispersed across various documents, the authorities demonstrated that their activities target the identified risks. At the time of the assessment, the impact of the mitigation measures taken as a result of the NRA was limited due to the recent adoption of the AP (four months before the on-site visit).

5. The FIU and the NBS have communicated the outcomes of the NRA to the financial institutions (FIs) and designated non-financial business and professions (DNFBPs) by conducting awareness-raising meetings and trainings and by publicising the NRA on their websites.

Recommended Actions

1. The authorities should conduct the next iteration of the NRA, which ought to:

   a. place an increased focus on serious threats, such as OC;

   b. comprehensively explores the full range of vulnerabilities such as beneficial ownership issues, use of cash (including cross-border transportation of cash), as well as potential misuse of legal persons. In light of evolving ML/TF risks, the NRA should also include a chapter on new technologies;

   c. be timely conducted and benefit from sufficiently broad sources of information, including reliable statistics and trends and typologies in ML/TF;

d. performs a more detailed analysis of FT risks based on FATF guidance, including risks of financing and misuse by terrorist organisations of NPOs and other types of legal persons;

e. includes the DNFBP sector in the NRA process and ensure that the results of the NRA are communicated to the DNFBPs. 2. Depending on the risks identified, authorities should strengthen their risk understanding of serious ML/TF threats and vulnerabilities.

2. The LEA policy measures in addressing the risk should be more granular in providing concrete measures to mitigate the risks and be better structured. The risk-based allocation of resources should be enhanced.

3. Slovakia should ensure a high-level political commitment in supporting AML/CFT policy development and in facilitating better strategic coordination. The operational coordination mechanisms should be revised to become more effective horizontally.

4. Better use the results of the NRA to justify exemptions and support the application of enhanced measures for higher risk scenarios or simplified measures for lower risk scenarios.

74. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1, 2, 33 and 34.

2.2 Immediate Outcome 1 (Risk, Policy and Coordination)

2.2.1. Country's understanding of its ML/TF risks

75. Slovakia has a moderate understanding of ML/FT risks, which derives mainly from the findings of the NRA. In case of supervisory authorities, the understanding of ML/TF risks is also based to some extent on the results of supervisory activities, information exchange with foreign supervisory authorities, supra-national risk assessment conducted by the EU, and in case of the FIU, the number and the content of the UTRs. The LEA's understanding of risk is based on practice and on the GPO's sectoral vulnerabilities assessment. Overall, the accuracy of the NRA impacts on country's understanding of risk.

76. The first Slovak AML/CTF NRA was officially completed in 2017 on the basis of statistics and other data collected for the period 2011-2015. The public version of the NRA report was drafted in mid-2017 and was subsequently published on the FIU website in mid-2018. The Government officially acknowledged the document on 7 May 2019 by binding resolution. Most of the competent authorities[26] and some private sector entities were involved in the process.

77. As already mentioned under Chapter 1, the AT has some concerns in relation to the accuracy and reasonableness of the conclusions of the NRA due to: i) the time gap between the statistical data used and the moment of the adoption of the report; ii) certain risks (including the use of fictitious companies, the Fintech sector, the use of cash and external threats), have not received a significant attention; iii) the NRA does not provide a comprehensive description of the main ML methods, trends and typologies. The national statistics system was considered as a limiting factor in the work of the NRA task force[27] with other evidence of inefficient data

[26] For instance, the judiciary was not involved in the process.

[27] Module 1 page 4 Non- public part of the NRA

management[28].

78. The authorities are aware that the pool of information and data used in the threat analysis was somehow limited to the content of ML convictions achieved (based on even older facts and criminal behaviour) and agree that the global understanding of risks should extend beyond those. This shortcoming was partly remediated by considering some of the on-going criminal procedures on ML and proceeds generating crimes. Nevertheless, there is a need of increased focus on external threats, organised crime, beneficial ownership issues and non-profit organisations (NPOs).

79. There is a significant time lag between the period for which the NRA was conducted (2011-2015), the period when the assessment took place (2016-2017), the timing of disclosure of its final results (2018), and the time when promulgating the AP to mitigate the identified risks (2019). According to the AML/CFT Act (see R1 under TCA) the NRA shall be updated to follow the development of risks of ML and TF, but no precise timelines are set therein. Nevertheless, the AP provides for an update of the NRA "generally" every four years.

80. NRA contains a public and a non-public version. The public part was disseminated between all parties who were engaged in conducting NRA, and to the private sector (in 2018) who started then using its results in their work. While the confidential section was not disclosed to the private sector, the opinion of the various bodies on the substantive added value of the non-public part differs. While the LEA (especially GPO) appear to make use of the elements included therein, the supervisors share the opinion that the non-public part is only a particularization of data already aggregated in the public section. Both the LEA and supervisors have a correct understanding and awareness of the findings of the non-public version.

81. The vulnerabilities at national level points to the authorities' ability to fight ML including insufficient staffing and financial resources of the FIU and the supervisors, lack of specialization in identifying and tracing of proceeds and in performing financial investigations. This results in difficulties in prosecuting serious autonomous and 3rd party ML cases and insufficient seizure and confiscation of proceeds of crime. Other, more granular shortcomings have been identified such as: the absence of a central bank account register; inefficient data management systems and statistical data, and lack of systematic training of LEAs and courts in the area of ML and proceeds recovery.

82. Overall, the NRA does not provide a full picture of the main methods, trends and typologies used to launder proceeds of crime in SR, which have an impact on LEA perception of those. To be more specific, the NRA concluded, and the practitioners confirmed that most of the proceeds are used for the immediate consumption by the perpetrator of the predicate offense, without specific elements of ML. This does not appear to be reasonable, nor fully in line with the reality. The acknowledged laundering methods are rudimental and consist of transfers to bank accounts followed by withdrawals in cash and sale of stolen objects to disguise their origin, with no sophisticated forms of legalization identified, *e.g.* using placement of proceeds abroad or by engaging professional individuals[29].

83. The authorities have a reasonable understanding of ML threat resulting from the misuse of companies, including through use of complex VAT frauds schemes and *"straw men"*. Nevertheless, certain ML-related risks have not received sufficient attention during the NRA process, and are less known by the authorities. For instance, the use of different types of corporate vehicles in criminal

[28] One of the "baseline" findings from the assessment process is that there is no plausible statistics available in the framework of the SR law enforcement authorities and judiciary that would express, in quantitative terms, the value of proceeds of crime with a satisfactory degree of veracity." - Module 1 page 87 Non-public part of the NRA

[29] Page 12 NRA

schemes, which is to a large extent linked to VAT frauds and trade-based ML, was not assessed to a great degree. In general, the ML/TF risks associated with legal persons have not been assessed sufficiently. Same goes with the cash movements across the country which were not sufficiently explored (see also the issue of BNI declarations in 2016 and 2017 as described under IO8.3)

84. The LEA understanding of risk is supplemented by the GPO sectoral vulnerabilities assessment carried out on its own initiative (in 2015). The resulting document, the *"Assessment of limits of efficiency of the activity of Prosecutor's Office in the area of criminal prosecution of money laundering and in seizing proceeds from crime"* identified a deficit in performing full-value proactive and parallel financial investigation and other shortcomings in the area of property seizure and criminal assets management. Therefore, the issue of ML criminal prosecution, seizures and final confiscation of proceeds from crime got into the centre of attention of the Prosecutor's Office. Subsequently, this document was submitted to the President of the Police Force and MoJ for further utilisation with the call to adopt measures to address those shortcomings not falling under the competence of the GPO.

85. The overall TF risk is understood as *"medium-low"* and has a dedicated chapter in the NRA. While not challenging the actual risk level, the AT believes that this conclusion might need reconsideration (up-date), taking into account the on-going TF cases (in which Slovak residents and financial institutions appear to be involved). The TF risk assessment lacks granularity and includes a listing of rather general TF related risk than a sound analysis of trends, sources, financial products and services that could be misused. Some potential TF risks appear not to be fully addressed, such as misuse of NPOs and the poor control on the cash movements across the country. Financial instruments such as virtual currencies and money remittances, as well as the use of fictitious corporate structures, may also pose a certain level of risk, which has been insufficiently explored.

86. Broadly, the TF risks are understood by LEA agencies, and investigators, prosecutors and intelligence officers appear to have the necessary skills and knowledge to identify, investigate and prosecute FT, should the need arise. The LEAs consider the non-dissuasive nature of sanctions in relation to undeclared/falsely declared movement of cash and the absence of a mechanism to trace the possible criminal origin of such cash when detected, as factors which could increase FT risks.

2.2.2 National policies to address identified ML/TF risks

87. To a large extent, Slovakia's national AML/CFT policies address the identified ML/TF risks. Although its policies and plans can be general and dispersed across various documents, the authorities demonstrated that their activities target the identified risks.

88. The main strategic document adopted to address the identified ML/TF risks is the *"Action plan for combating money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction for the period 2019 – 2022"* (hereafter AP)**,** which provides for *"orders"* and *"recommendations"* with particular deadlines for specific Governmental authorities. The *"orders"* appear to be binding and are limited to the Ministries (MoI, MoJ, MoF, Ministry of Defence, MFA) while the *"recommendations"* apply to the GPO and the NBS.

89. The Office of the Government monitors the execution of the AP tasks through an electronic system. For *"continuous"* task, the monitoring is done twice per year. For time-determined tasks the respective ministry must report electronically or in paper form if and how the task was fulfilled. In case one task is not completed, the reasons must be explained and an official request for a prolongation must be submitted. The FIU is responsible to collect all the reports on the AP tasks from all responsible institutions (*e.g.* NBS) and forward them in a consolidated manner

through the chain of command (Office of the Police President, MoI) to the Office of the Government.

90. Some of the orders and recommendations are general and do not have a direct applicability in practice (*i.a.* to reduce the level of social acceptability in the area of generating illegal proceeds), while others are easier quantifiable in terms of results (*i.a.* to submit a draft law on the enforcement of decision on seizure of property and on the administration of seized property).

91. The AP contains a broad list of measures which correctly address the vulnerabilities identified in the NRA, such as: introduction of proactive parallel financial investigations in ML cases; organization of trainings and workshops for the FIU; raising awareness of obliged entities on their AML/CFT obligations through training methodological documents; enhancing the comprehensiveness of statistics kept by the FIU; updating the NRA; development of typologies and sophisticated ML schemes using of legal entities, cross-border operation and implication of tax havens etc…

92. While welcoming the adoption of the AP, the shortcomings of the NRA impact the capacity of the national policies to fully address the ML/TF risks. The AT acknowledges the steps taken by the authorities in the application of the AP, but due to its recent adoption (four months before the on-site visit) the effectiveness of actual mitigation measures implemented was difficult to assess.

93. At the GPO level, the document *"Measure of the GPO, implementing the NRA, the strategic principles (2019 – 2024), and the AP"* was adopted in June 2019 (hereafter the GPO Measures). The document contains 21 *"Special tasks"* given as responsibilities for various Departments of the GPO or to the prosecutors in general. The GPO Measures is a relevant policy document in the context of the identified ML/TF risks and it is binding for all prosecutors. Nevertheless, the GPO policy measures in addressing the NRA should be more specific in providing concrete measures to mitigate the risks and be better structured. No concrete results could be presented to the AT due to recent adoption of the document.

94. To address the deficiencies identified in relation to the transparency of legal persons, the Register of UBO, administrated by the Slovak Statistical Authority, was created. This is a measure in line with the country risk. The legal persons and arrangements should have provided information about their BOs by 31st December 2019.

2.2.3. Exemptions, enhanced and simplified measures

95. The only exemptions in the application of the FATF requirements pertain to CDD. As detailed under R1 (see TCA) the CDD exemptions are not justified by the NRA. Nevertheless, the AML/CFT Act does include risk-based mitigation measures as it applies only to: i) electronic money which cannot be deposited repeatedly, and the maximum amount will not exceed EUR 250 or EUR 500 for use only on the territory of SR and ii) payment services provided through the public electronic communication network provided that the value of one transaction does not exceed EUR 30 and, simultaneously, the total monthly limit of payments made from one telephone number does not exceed EUR 250. The payment devices can be used exclusively for purchases of goods and services and they cannot be funded by anonymous electronic money. The exemptions cannot be used in case of reverse exchange of cash or cash withdrawal of an amount exceeding EUR100. The obliged person shall monitor the transactions or business relationships so that it is possible to detect an unusual business operation. None of the FIs met on-site made use of those exemptions.

96. When applying the CDD measures, the REs shall consider the risks, including those identified at the national level. Overall, the AT found that the results of the NRA were not always used for revising the ML/TF risk assessments by the private sector, but the conclusions on the

country risks prepared by the individual RE (especially larger FIs) go in the same direction, or are even more accurate and detailed than the NRA.

97. Enhanced CDD is applied risk based and regulation based. On one hand, the AML/CFT Act provides for obligatory ECDD measures in certain pre-determined scenarios such as cross-border correspondent relationship or for PEPs. On the other hand, the REs must determine the risk and the basis of their own assessments. In practice, the risk assessments of the FIs appear to be reasonable. The DNFBPs are more leaning on the regulation-based cases provided by the AML/CFT Act rather than on the sector-tailored risk assessments.

98. The application of the SCDD measures is allowed but the scenarios presented in the AML/CFT Act do not directly steam from the NRA. Nevertheless, in practice, simplified measures are not applied by banks and by most the DNFBPs. Only a handful of non-banking FIs and casinos apply simplified measures.

2.2.4. Objectives and activities of competent authorities

99. Objective setting measures have been applied as a result of the NRA such as the adoption of the AP, and the GPO Measures which list a set of tasks in the implementation of the NRA and other strategic actions. While both documents are consistent and address the risks identified, more clear indicators to measure the effective implementation is still needed, to make sure that the actions remain aligned with the evolving national AML/CTF policies and with the ML and TF risks identified. No other objective-setting documents has been reported.

100. Steps have been taken at the GPO level to address the vulnerabilities identified in the course of the NRA (2018) or in the context of the *"Assessment of limits of efficiency of the activity of Prosecutor's Office in the area of criminal prosecution of money laundering and in seizing proceeds from crime"* (2015). The later was done at GPO's own initiative and it is the first document assessing threats and vulnerabilities in the area of AML/CFT targeting to produce substantive change of thinking amongst LEA.

101. A good example of specific activities which address identified risks, is the *"Conclusion and measures"* document approved[30] by the Deputy GPO following a joint working meeting on *"Financial investigation in criminal proceedings"* which foresees: i) the adoption and implementation of a "Methodological tool of financial investigation" by the bodies of Presidium of the Police Force and the General Prosecutor´s Office; ii) the preparation of a legislative framework for financial investigations; iii) the establishment of the central registry of bank accounts; iv) drawing up proposals for modalities of introduction of the reverse burden instrument in proving proceeds of crime and the application of extended confiscation; v) drafting proposals for a change in the field of seized property management and execution of confiscation decisions (AMO); vi) pursue systematic education programs. As an immediate result, the Methodical Guidance on Financial Investigations was adopted by the Presidium of the Police Forces in 2017, and some steps have been taken for the creation of the establishment of the central registry of bank accounts which is unanimously considered by LEA as an important element in conducting more effective financial investigations. The rest of the instructions were not followed by actions.

102. On the occasion of the annual meeting of the GPO with regional prosecutors held in September 2018, both the SPO and regional prosecutors were ordered to conduct financial investigations in all criminal matters in which the CC sets out the forfeiture of property as an obligatory punishment; and in all pending ML cases where the predicate offence concerns

[30] 8 November 2016

corruption, abuse of office, serious fraud, financial and tax crimes, or organised criminality. The General Prosecutor and the Deputy General Prosecutor for Criminal Matters Department had to be informed on the progress in this field.

103. While welcoming the above described initiatives (and similar others, the most recent dating from 25 July 2019) taken by the GPO and Police Forces to address some of the identified national vulnerabilities, the AT perceives a certain dissipation of the various messages and instructions in oral and written guidance/directives, all lacking structure and sometimes enforceability. Another weak point is that all efforts made at the LEA (mainly Prosecution) level are geared towards the vulnerabilities ignoring the threats. Therefore, measures to address the risk scenarios and to orientate the authorities' objectives such as ML typologies, guidance in investigating various types of ML, or a case prioritization system, are absent.

104. The Police Forces contributed to streamlining the financial investigations by adopting the Methodical Guidance on Financial Investigations in 2017. However, the NRA did not lead to important reforms, and during the on-site interviews the LEAs could not demonstrate how they prioritise their cases to address particular risks identified in the NRA (for example corruption related ML cases).

105. The NRA conclusions were adequately incorporated in the Methodical Guidance for individual sectors of the financial market, into supervision procedures. The NBS as a supervisory authority monitors the situation in the area of new or newly occurring risks – *e.g.* in using new technologies and procedures such as the identification and verification of client without their physical presence in the financial institution (in 2019, the NBS published on their website an opinion on the topic which applies for banks). The practical application is checked during the on-site visits to banks.

106. The NBS actively monitors the FinTech area and shares information with the Centre for Financial Innovations of the Ministry of Finance. The NBS has established the Innovation Hub as a mean to enter into dialogue with the FinTech sector and present the bank's opinions on questions submitted by interested persons within NBS's competence.

107. The results of the NRA are considered by the FIU when performing supervisory activities according to the *"Methodological Guidelines for Inspections"*. Turning to the core-functions of the FIU, the *"Methodology for implementation of the AML/CFT Act"* include a categorisation of UTRs based on risk. On a less positive side, the criteria allocating the UTR into the risk categories are rather general, such as postponed transactions, persons already under analysis or existence of TF suspicions, and do not consider the particular ML risks Slovakia faces. At strategic level, more typologies work is needed to enhance understanding of risk, to ensure more consistency of objectives and activities of the FIU with the evolving ML/FT risks.

2.2.5. National coordination and cooperation

108. The Slovak Republic has established a good foundation for national coordination and cooperation in criminal matters. MEKO is a long-established and effective group for strategic coordination between relevant authorities. Under the coordination of the MoI, the following authorities are part of the MEKO: GPO, SIS, Police Forces, the Court Guards and Prison Wardens Corps the Military Police Military Intelligence; Department of Fight against Frauds of the Financial Directorate; Financial Administration Criminal Office, MoJ, MoF (Customs Department), and Civil Aviation Section of the Ministry of Transport and Construction.

109. MEKO's objective is to harmonize and streamline the activities of all police, security and intelligence units, prosecutor's offices and key government bodies in the area of combating

terrorism and organized crime. MEKO collects and evaluates initiatives of ministries, other central administration bodies, organizations and institutions, adopts opinions, proposes measures and assesses their effectiveness. It initiates legislative proposals and other regulatory measures to fight against crime.

110. MEKO holds regular meetings and advises the Council of the Government for Criminality Prevention (the Council). In turn, the Council submits initiatives, recommendations and proposals to address the emerging trends, threats or other issues identified by MEKO and other relevant stakeholders. The Council's representatives are present in the MEKO annual meetings. The Council approves all strategies developed by the competent authorities in the area of crime prevention.

111. To ensure the operational cooperation and coordination, by Resolution of MEKO from 16 May 2002 a *"Multidisciplinary integrated group of experts focused on the elimination of money laundering"* NES-LP was established. After the adoption of the AML/CFT Act in 2008, the scope of competence of the group was extended to the area connected with protection against terrorist financing. In 2017 the scope of NES-LP was extended to PF issues but only one targeted meeting was held since. The communication with MEKO is done vertically. In case horizontal issues are identified those shall be communicated to MEKO who will inform the respective specialised sub-group.

112. The FIU Director is the leader and the NES-LP which includes NBS, MoF, the Presidium of the Police (Anti-Corruption, Anti-Drug, Financial, Counter-Terrorism and Criminal Counter), the Police College in Bratislava, FACO, MoJ, GPO, SIS, Military Intelligence, Ministry of Economy, MoF and FDSR. The objective of the group is to propose a suitable way of exchanging operational information on ML and TF, to coordinate the activities in order to avoid duplications in solving individual cases, and to be a platform for operational information exchange on ML and TF cases and suspected persons and companies.

113. As it has been identified in the NRA's vulnerability analysis and reflected in the relevant part of the AP, the authorities are aware of the limits the AML/CFT national coordination system and its ability to set and effectively monitor long-term policy objectives, cooperate horizontally and enforce the strategic decisions adopted. In particular, more coordination and cooperation at strategic level is needed to ensure more efficient application of the TFS regime.

114. The key players within the CFT framework are the Counter-Terrorism Unit NAKA (CTU-NAKA), the FIU, Slovak Information Service (SIS), Military Intelligence (MI) and the Special Prosecutor Office of the General Prosecutor's Office (SPO). These entities coordinate and cooperate on a continuous basis in the fight against terrorism and terrorist financing, in several forms. Among others an *Interdepartmental Expert Group on Coordinating of the Exchange and Analysis of Information and Cooperation in the Fight against Terrorism* has been set up and meets at least four times a year to assess the current issues of fight against terrorism and terrorist financing. The expert group assesses the measures under the *National Counter-Terrorism Action Plan (2015-2018) (CT-NAP),* which is regularly up-dated (every four years).

115. At operational level, the domestic cooperation in TF-related investigations and pre-investigative operative analyses has been facilitated since 2013 by the establishment of the *National Security Analytical Center (NSAC)*, as an analytical, communication and coordination workplace with nationwide coverage in the security area. NSAC is composed of representatives of the SIS, MI, Police Force, FACO, MFA, General Staff of the Armed Forces, National Security Authority and Government Office. The AT notes the absence of the FIU from the NSAC composition. On a positive side, the NSAC's activities are sometimes supported by the FIU, although its' staff is not present in the meetings. Coordination between NSAC and FIU or other competent unit of the Police

Force is done via the Police Force´s representative.

2.2.6. Private sector's awareness of risks

116. The FIU and the NBS have communicated the outcomes of the NRA to the financial institutions (FIs) and designated non-financial business and professions (DNFBPs) by conducting awareness-raising meetings and trainings and by publicising the NRA on their websites.

117. Private sector stakeholders are generally informed about AML/CFT risks. This awareness-raising exercise was carried out by relevant authorities, including NBS through their Institute of Banking Education (IBE). IBE in cooperation with the Banking Association for Central and Eastern Europe organises the international AML conference on yearly basis, and CFT workshops in cooperation with UNODC.

118. During the on-site visit it was determined that IBE trainings are useful mostly for the beginners in AML/CFT field and less for more advanced and skilled staff operating in the banking sector. More sophisticated trainings are necessary for the AML/CFT specialists who need specific and current information to deal with the daily problems they face. Almost 3 000 persons per year take part in AML/CFT trainings all from financial institutions, with no representatives of the DNFBPs sector. This fact raises concerns, whether DNFBPs sector aware enough about the ML/TF threats and vulnerabilities and are prepared to cope with relevant issues.

Overall conclusion on IO.1

119. Most of authorities' understanding of risk is based on the results of the NRA, therefore the deficiencies there identified impact on the overall risk perception and appreciation. The prosecutors have a better understanding of the specific risks which go beyond the NRA and do take into account more serious and current threats, such as organized crime, cybercrimes and corruption. The LEA have a fairly good understanding of TF risks while the other authorities have only a general awareness of those. In case of supervisory authorities, the understanding of ML/TF risks is also based to some extent on the results of supervisory activities, information exchange with foreign supervisory authorities, supra-national risk assessment conducted by the EU, and in case of the FIU the number and the content of the UTRs. Existing CDD exemptions, enhanced and simplified measures provided by the AML/CFT Act are risk-based although not fully supported by the NRA. The overwhelming majority of FIs and DNFBPs do not apply the exemptions and simplified CDD measures. The objectives and activities of the competent authorities are consistent with the evolving national policies and plans, although the relevant documents are lacking structure and in some instances enforceability. Slovak competent authorities have the necessary mechanisms to cooperate and coordinate at operational and policy level to combat ML and TF, with more efforts needed in the policy coordination for the implementation of the TFS. The FIU and the NBS to a large extent ensure that FIs and DNFBPs are aware of the NRA results by publishing this information on their websites and providing awareness-raising meetings and trainings.

120. **The Slovak Republic is rated as having a Moderate level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

3.1 Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

1. The Slovak legislation provides LEAs and FIU with an adequate legal base to collect and use financial intelligence both domestically and internationally. The sole written instructions on conducting financial investigations at police level is the Methodical Guidance issued by the Presidium of the Police Force in 2017.

2. The LEAs making more use of the financial intelligence are the Financial Police Unit NAKA and ARO NAKA while the use of financial intelligence by other Police Forces is minimal. The absence of a bank account register, together with the lack of BO register were reported as the greatest challenges in conducting financial analysis. While there are some positive results, overall, FIU products are not successfully utilised by LEA in ML cases. SR has weak results both in terms of ML investigations conducted based on FIU disseminations, and, more generally, in using financial intelligence and other relevant information to develop evidence and trace criminal proceeds related to ML. However, LEA have exploited the FIU's intelligence packages for investigations into predicate crimes.

3. While the FIU analysts met on-site were knowledgeable and have the ability of producing complex analysis, there is insufficient coherent management at the FIU level to gear their activities into becoming more effective. In most cases, the FIU products are not successfully utilised by LEA in ML cases. At best, LEA exploit them for investigations into other crimes than ML.

4. The FIU's dissemination system dissipates its resources into less relevant cases, often not related to ML. This has a negative impact on the quality of the analysis and on the FIUs operational independence. Too many FIU products are sent to the Financial Directorate of SR to be used for tax audit purposes.

5. There is an absence of LEA specialisation in obtaining and exploiting the financial information/intelligence, rather than shortage of legal means and/or opportunities. NAKA units lack internal cooperation and coordination in this respect and the police officers are not sufficiently motivated to engage in financial intelligence work. The Regional PF and other Police bodies have not demonstrated sufficient results in using financial intelligence, despite the volume of FIU disseminations received.

6. Overall, the FIU receives a reasonable number of UTRs although their quality varies. The authorities are unanimous in saying that the private sector's reporting on TF is adequate and the number of UTRs does not pose a significant burden on the FIU work. The FIU started to improve the feedback given to the RE. The process of categorisation of UTRs places almost 90% of the reports under the higher risk categories, which is not sufficient to effectively prioritise the UTRs.

7. FIU does strategic analysis only in the context of the annual reports. Limited efforts have been made to raise awareness of LEA on the findings of the annual reports with a view to use the conclusion in their activity.

8. At the international level the FIU is active and responsive. There are no requests from foreign counterparts which remained un-answered and the feedback provided by the international community regarding the Slovak FIU was generally positive.

9. Turning to TF, the FIU products are examined by the competent LEA, and financial intelligence is routinely collected and used in TF investigations.

Immediate Outcome 7

1. The number of investigations and prosecutions for ML are on the rise, although the law enforcement and judicial practice could not demonstrate that the fight against ML activity was a priority objective for the entire evaluated period. ML is mainly analysed together with the predicate offence on which the investigation is centred.

2. The ML offences are identified and investigated by the authority having competence over the predicate offence as there is no dedicated LEA for ML crimes. The assessors note that LEAs collect information on predicates in the operative pre-investigative proceedings but do not appear to always pay due attention to the identification of proceeds and to associated ML activities. There is lack of timeframes and insufficient controls in the pre-investigative stage which leads to lengthy proceedings (especially when considering the moment of the perpetration of the crime and the moment of the conviction).

3. Parallel financial investigations have been performed since 2017 upon the Methodical Guidance issued by the Presidium of the Police Force, but in practice such are not conducted on a systematic basis.

4. Since 2013 the number of final ML convictions increased to an overall number of 58 (94 persons), the majority pertaining to simple property crimes such as car thefts. All types of ML convictions have been achieved (self-laundering, third-party and autonomous ML), including laundering of foreign proceeds. While legal entities are said to be frequently used as vehicles for legalisation purposes, no legal person has been convicted for ML so far, with some on-going investigations reported.

5. The outcome of investigations and prosecutions of ML do not appear to fully reflect the country risks. The AT is not convinced that the LEAs are currently in a position, due to several factors including resources, to effectively and timely investigate and prosecute high-level and complex ML cases. Same convictions for ML related to organised crime, human and drug trafficking were reported, but remain modest, while tangible results in prosecuting and convicting corruption related ML cases have not been achieved.

6. The sanctions applied for ML offences, which mainly consist of custodial sentences and fines, appear to be proportionate. The level of dissuasiveness of the sanctions imposed is mirroring the profile of the convictions achieved so far, which are rather simple ML cases. The average sentence for ML is of 32 months. The AT is confident that enhancing the profile of the ML into more serious and complex cases will lead to the application of more dissuasive penalties.

Immediate Outcome 8

1. The frequent use of provisional measures constitutes a commendable progress in the overall system. However, it does not appear to be followed by the performance of the confiscation regime. From the limited information made available to the assessors, the confiscation measures are rarely if at all imposed in criminal cases and only a fragment of the secured assets is finally

confiscated.

2. The effectiveness of the provisional measures applied in financial investigations is seriously affected by the lack of proceeds-oriented operative analysis in the pre-investigative proceedings, the logistical and procedural constraints at certain LEAs, the (putative) limitations to seize assets from third parties, and the high evidentiary burden required for certain provisional measures.

3. There are some procedures, but not comprehensive and effective mechanism for the managing and/or disposing of property that is seized or confiscated and neither is there any centralized body in charge of management of such property, bearing a direct impact on effectiveness particularly if more complex types of assets have to be managed.

4. The cross-border cash control regime has not demonstrated its effective applicability to detect ML/TF related cash/BNIs transported through the borders of the Slovak Republic that also constitute external borders of the EU. In the few cases of false or non-declaration, no assets were restrained and there is no mechanism available to counter cash couriers entering through the EU internal borders.

5. The absence of comprehensive and sufficiently detailed statistics poses an impediment to assessing the performance and effectiveness of the confiscation regime and the actual recovery of confiscated assets.

Recommended Actions

Immediate Outcome 6

1. The financial aspect should be systematically explored by all LEA involved in investigating ML and proceeds generating crimes to: i) target ML and FT elements; ii) follow the trail of potential proceeds; and iii) identify other involved parties (such as beneficiaries of transactions).

2. The specialization of all LEA actors in the field of collecting and use of financial intelligence should be enhanced and the police officers should be better encouraged to engage in financial analysis in ML and proceeds generating cases. The access to databases and registers should be integrated and enhanced.

3. The FIU staff should be properly motivated and the FIU should be provided with stable and competent management.

4. The FIU should reconsider the dissemination system to ensure focus on the strong ML and FT suspicions, coupled with meaningful analysis to support the operational needs of LEA. Ambiguous provisions on FIU disseminations should be eliminated or clarified, to avoid potential threats to the FIU operational independence and confidentiality requirements.

5. At strategic level, the FIU should enhance awareness amongst public authorities and LEAs on the overall FIU work and its role in the AML/CFT system. The FIU strategic analysis should be enhanced and should include ML typologies.

6. Prosecution and LEA should provide effective feedback to the FIU, to enhance the quality of the disseminations and to detect challenging areas.

7. Measures should be taken to improve internal cooperation and coordination of NAKA units in timely obtaining and exploiting the financial information/intelligence (including *i.a* setting

up a system for management of internal requests).

8. The authorities should undertake outreach activities (including providing specific feedback to REs) to enhance the quality of the UTRs.

9. The Customs should enhance ML/TF knowledge and develop sound mechanisms to be able to detect false or non-declarations and suspicions of either ML or FT (which could arise even where declarations are submitted).

Immediate Outcome 7

1. Slovakia should streamline the existing law enforcement guidance/instructions by developing a ML-specific operational tool which should:

a. clearly set out how each LEA identify and initiate ML cases at the earliest stages of suspicion using the best investigative techniques in a coordinated manner, to trace the sources and destination of proceeds of crime;

b. introduce the obligation to pro-actively conduct and coordinate parallel financial investigations in all proceeds-generating cases, pursuing the *"follow the money principle"*, both at operational and pre-trial stages.

2. The ML investigation policy should be more consistent with the ML risks that the country faces, as highlighted in this report and from the reviews of the ML-related criminality patterns. LEAs should target more complex and sophisticated types of ML such as cases involving organised crime (drug, human trafficking), corruption, foreign predicates. When fictitious companies are used, LEAs should extend their investigation to identify the person(s) who ultimately controls and benefits from the scheme.

3. LEA should be provided with on-line access to various DBs and with tools to swiftly integrate the search results into an analytical product.

4. The authorities should take measures to ensure that the operational (pre-investigative) phase is proceeds-oriented and not open-ended. Clear formal rules on which a pre-trial ML investigation is undertaken should be adopted, ensuring an effective monitoring of the results.

5. In order to develop a more proactive approach to ML investigations and prosecutions, the law enforcement bodies and the GPO should challenge the judiciary with more cases where it is not possible to establish precisely the underlying offence(s) but where the courts could infer the existence of the predicate criminality from adduced facts and circumstances.

6. A national ML-specific enforceable operational policy is needed to ensure a more uniform and effective approach across all LEAs involved. Comprehensive training on financial investigations should be provided regularly to the Prosecution and law enforcement staff, (particularly those responsible for major proceeds generating offences) and the judiciary.

Immediate Outcome 8

1. LEAs should be provided with the necessary resources (in terms of either additional staff or more specialized units) to perform broad, proactive and effective parallel financial investigations to identify and secure criminal proceeds.

2. Extensive training should be provided to LEAs so as to enhance their knowledge of the possibilities provided by the existing legal framework of the confiscation and provisional measures

regime (*e.g.* in the field of third-party seizure and confiscation).

3. The Slovakian authorities should seek for legislative or other solutions to effectively overcome the apparently overly high evidentiary burden attached to certain provisional measures in the CCP (e.g. Art. 425 et al.), especially in case of-third party confiscation regime.

4. The authorities should review the framework for forfeiture/confiscation to identify the possible issues in the process and take appropriate steps to ensure that criminal proceeds are confiscated in all cases.

5. Comprehensive statistics should be kept and maintained regarding the performance and volume of the provisional measures and confiscation regime as well as the assets that have actually been recovered.

6. A comprehensive mechanism should be adopted for the managing and preserving the value of complex assets that have been seized or confiscated, for which the mere safe-keeping measures are not sufficient, preferably by introducing a centralized body in charge of management of such property.

7. Technical deficiencies under Recommendation 32 should urgently be remedied, particularly as regards the lack of Customs powers to stop or restrain cash/BNIs in order to ascertain whether evidence of ML/FT may be found. Together with this, measures should be taken to ensure that control of cross-border transportation of currency (at least through EU external borders) also takes into consideration identifying ML/FT suspicions and the Customs authorities include in their focus the identified risks also in terms of detecting cash smuggling and seizing falsely declared cash or BNI according to the known risks.

121. The relevant Immediate Outcomes considered and assessed in this chapter are IO.6-8. The Recommendations relevant for the assessment of effectiveness under this section are R.1, R. 3, R.4 and R.29-32.

3.2. Immediate Outcome 6 (Financial Intelligence ML/TF)

122. For most of the evaluation period, the FIU of the Slovak Republic was a part of NAKA. There was no clear demarcation in the level of decision between the FIU and the other NAKA units. This position of the FIU raised serious questions on the independence of the FIU at the time of the previous round of mutual evaluations.

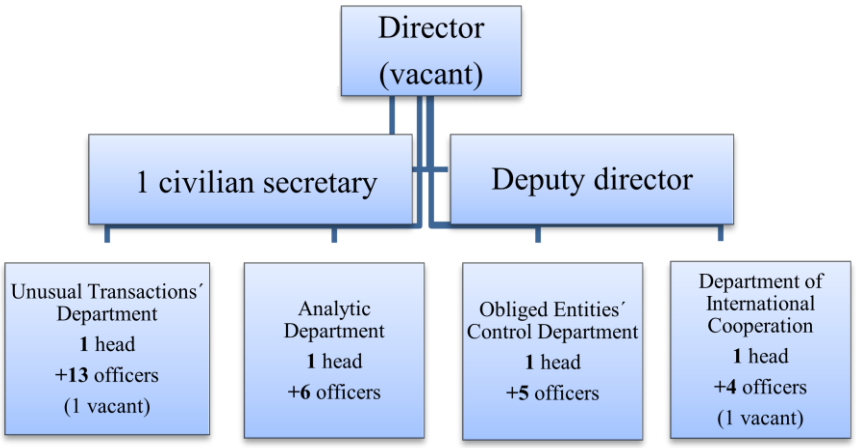
123. The situation changed shortly before the on-site visit, in August 2019, when the FIU was put under the direct supervision of the President of the Police Forces. That places the FIU one step higher in the Police structure with the intent of increasing its level of independence by having its own budget item, and by giving the FIU Director the power to employ staff on its' own decision. Nevertheless, the number of FIU employees, the level of their salaries and their ranks remained the same. The re-structuring was not considering the emerging needs of the FIU in terms of potential additional staff needed. Due to recent re-structuring, the AT was not able to measure the actual impact this measure on FIU's activity.

124. At the time of the on-site visit the FIU had 37 positions (including management positions) out of which 33 were filled-in with personnel. Recruitment difficulties have been reported by the authorities due to lack of experience on the FIU specific work amongst police officers and low motivation. In the last five years there was an abnormal turnover of appointed FIU Directors,

which confirms the absence of safeguards in this regard. At the time of the on-site visit, the FIU did not have an appointed Director since March 2019.

3.2.1. Use of financial intelligence and other information

Picture 1: FIU organisational chart



125. The FIU, as a part of the Police Force has access to a number of databases (DB) through the NetReveal analytical system which integrates: the Investigation files log (data on finalised and on-going criminal cases), the Commercial Register, the Population Register, the register on companies bank accounts kept by the Financial Directorate, and Data from Document Management System (DMS). The DMS is internally created and managed, containing information about the FIU cases, including UTRs and spontaneous disseminations, and information requests from foreign counterparts.

126. NetReveal is completely cut-off from the Internet, the external BDs being up-loaded quarterly on the FIU server. If in the course of verifications an analyst has suspicions that some information might be out-dated (changes occurred between the last up-load and the moment of the check) he/she can double-check by performing the search in the on-line DB using a separate work station connected to the Internet (*i.a.* the fiscal declarations can be obtained from www.finstat.sk if needed). The FIU does not have access to paid international BD.

127. Apart from facilitating the search in multiple BD in one-click, NetReveal is a visualisation tool, which generates schemes and links between various subjects. When completing the analysis, the FIU uses publicly available sources and makes requests for additional information if need be.

128. In addition to NetReveal and upon request, the FIU has access to information from LEA's operational cases and from the obliged entities. The LEA's operational cases need to be accessed separately, as they are not yet up-loaded in the investigation files log before the launch of the investigative phase. In case of banks, the information requests are sent, and the replies received electronically, using the same secured channel as for the UTRs. For the rest of the REs, the communication is done through classic mail. In case the bank accounts of the suspected person are unknown, in the absence of a bank account register, the FIU shall file requests to all banks in Slovakia. This constitutes an additional burden for the FIU work.

129. The legal framework for financial intelligence gathering by LEA is underpinned by the Act on Police Force, the AML/CFT Act and the CC depending on the stage of the procedure (see also IO7).

The sole written instructions in the area of financial investigations is the Methodical Guidance issued by the Presidium of the Police Force in 2017, which however, cannot be considered enough to assist the LEAs in conducting effective and systematic financial analysis and investigations. Overall, the legal base for collecting financial intelligence for investigating ML is appropriate, but not equally understood and applied.

130. The LEAs making more use of the financial intelligence in ML and proceeds generated cases are the Financial Police Unit NAKA and ARO NAKA. The use of financial intelligence by other Police Forces (see list in IO7) is minimal. The Criminal Office for Financial Administration (FACO) routinely performs financial analysis and receives an important number of FIU disseminations, but those are used for tax related investigations rather than for ML.

131. The Police have direct access, without prior notification, to a number of registers and databases including commercial register, population register, vehicle records, real property register, vessel register, aircraft register and intellectual property right register (Copyrights, Trademarks, Patents, Designs and Industrial Rights). Information on fiscal declarations can be obtained upon written request from the responsible body of the MoF. In addition, international data from INTERPOL, EUROPOL, SIRENE are available and used.

132. Turning to financial information, LEA can obtain it either through the intermediation of the FIU or directly from FIs (in case of suspicions of ML or tax offences). In case of requests filed to the FIU, only data already held in the DMS will be provided. For bank statements and other financial information, requests are sent to the private sector, based on the Act on Police or on the CC, depending on the stage of the investigation. While the FIU is legally unable to be an intermediary between LEA and the FIs, some consideration should be given to the possibility for the FIU to obtain financial information on behalf of LEA in very serious cases. If case such option will be adopted, it needs to be doubled by a proper regulation, with safeguards in place to exclude any form of abuse.

133. The shortcoming related to the absence of a Central register of bank accounts apply to LEA as in the case of the FIU. In addition, the LEAs deplore the delay in which they receive the necessary data from the private sector, which often goes beyond the 30 days foreseen by the legislation. Most of the LEA have insufficient on-line access to DB and no connectiveness amongst them, which rends their work unnecessarily time consuming.

134. Overall, the AT does not see any impediments encountered by LEA in accessing financial intelligence and other information to develop evidence and trace criminal proceedings and ML. The limited results in this regard, appear to be caused more by an absence of LEAs awareness and capacities (including specialised human resources) in exploiting the financial information rather than shortage of legal means and/or opportunities.

3.2.2 UTRs received and requested by competent authorities

135. The FIU acts as the central authority that receives analyse, evaluate and process UTRs. During the period under review, the FIU has received a total of 19 520 UTRs, which are predominantly submitted by banks. The number of UTRs filed by the DNFBPs remains comparably low. Since 2015 an overall lowering trend in the number of UTRs can be noticed. According to the authorities, the FIU recently started to provide feedback to banks, leasing companies and gambling operators on the quality of the UTRs which might be a reason for the decrease in the number of reports submitted resulting in a stricter filtering of reports. Apart from the figures below published in the FIU annual reports, there is insufficient feedback provided to the rest of the private sector.

Table 8: Number of UTRs filed by RE

Reporting entity	2013	2014	2015	2016	2017	2018	06.2019
Banks	3 347	3 343	2 939	3 071	2 550	2 332	1 310
Building Savings Banks	67	34	14	5	3	1	5
Insurance	148	175	112	65	15	14	11
Securities	3	20	4	4	9	6	3
Investment and management companies	38	64	31	48	7	11	4
Exchange offices	0	8	9	5	1	0	4
Payment institutions, e-money	11	7	9	30	29	21	15
Financial leasing	45	35	27	18	9	9	7
Faktoring, forfaiting	2	1	1	0	0	0	1
Financial agent, consultant	2	0	0	0	1	0	0
Casinos, gambling games	12	3	20	15	2	106	10
Real estate brokers	3	2	0	0	0	0	0
Precious metal / stone traders	0	0	0	0	0	0	0
Lawyers, Notaries	16	1	3	8	4	4	0
Post company	105	108	55	22	3	2	0
Trade and service broker	81	127	38	6	3	3	2
Auditors / Accountants	4	0	1	0	0	0	1
Executors	1	0	1	0	0	0	0
Auction, rental	1	0	0	0	0	0	0
Trust and Company Service Providers	0	0	0	0	0	0	0
TOTAL	**3 886**	**3 928**	**3 264**	**3 297**	**2 636**	**2 509**	**1 373**

136. Between 2014-2017, the FIU received 341 UTRs from the NBS. The authorities explained that most of those were currency exchanges made in the context of the conversion of the national currency to EURO, and the grounds for suspicion were the relatively high amounts exchanged. In the absence of threshold reporting system, the NBS submitted those as UTRs.

Table 9: UTRs received from the NBS

Year	2014	2015	2016	2017	2018	06.2019
Number of UTRs	126	77	79	59	53	69

137. From the banks, the FIU receives the UTRs through encrypted e-mail communication, using secured channels, which allows only the qualified user to access the content of the message. The same channel is used for additional information request/replies. All information obtained from UTRs is stored in the FIU's DMS.

138. Overall, it appears that numerically the UTRs have reached a relatively stable and reasonable level. On a less positive side, the AT is of the opinion that the quality of the suspicious expressed in the reports is insufficient and does not fully correspond to the ML risks the country faces. In some instances, the suspicions are superficial and do not contain essential information on businesses or business relationships or are linked to mistakes in the customer identification. An element that could bare a risk on the private sector's appetite to report, is the too wide legal basis to disseminate, as described under R29.5. Examples of such is the important number of UTRs disseminated to the FDSR, and the disseminations made according to Art. 26 (3) of the AML/CFT Act.

139. Turning to TF UTRs, the FIU received an average or 96 reports per year with insignificant variations year by year (see Table 10 below). The authorities are unanimous in saying that the private sector's reporting on TF is adequate and the number of UTRs does not pose a significant burden on the FIU work. Th AT agrees on the latest as the TF related UTRs represented less than 3% of the total number of reports[31] received by the FIU between 2013 and 2018. The TF UTR analytical process is similar to the one applied in ML cases as escribed under *"operational analysis"* below.

Table 10: Number of TF related UTRs received by the FIU

RE	2013	2014	2015	2016	2017	2018
Banks	86	59	74	85	130	98
Insurance	-	5	-	-	-	2
Payment institutions and e-money	-	-	-	3	6	12
Investment and management companies	-	-	-	-	2	4
Casino	-	-	-	-	-	2
Post	-	-	-	1	-	-
Trade and service brokers	2	3	2	2	-	-
Total/year	88	67	76	91	138	118
Total (2013 – 2018)			**578**			

140. As an EU member state, Slovakia has established a cash declaration system for incoming and outgoing transportation of cash and BNIs over EUR10 000 across the external borders of the EU by natural persons. The completed declaration forms as well as notifications on any infringements of the reporting obligation are submitted to the FIU on a monthly basis, *i.e.* by the fifth day of the next calendar month. The movement of cash or BNIs by mail or cargo are not subject to any declaration or disclosure obligation.

141. The number overall number of cash declaration is modest (see Table 35 under IO8.3) and does not constitute a remarkable source of financial information for the FIU. Incoming currency declarations is higher than the outgoings, which appears to confirm the Customs' opinion that in most cases, the purpose of cash transport is mainly to acquire movable property (such as motor vehicles) or real estate.

142. Customs are not obliged to report suspicious movement of cash and hence they have no UTRs reported to the FIU. During the on-site interviews the Customs representatives did not display an adequate level of knowledge regarding possible suspicion of ML/TF related to cash transportation and the measures to apply in such situations.

143. The LEA have access to the information included in the UTRs based on case-by-case request addressed to the FIU. Statistics (see Table 11 below) demonstrate that the FIU avenue of obtaining financial information is regularly used, mostly to obtain data from abroad. In the latter situation, the subjects in the LEA´s request are searched within the FIU´s internal system DMS and in case of a positive relevant result, this is then submitted to the LEA together with the response provided by a foreign FIU.

144. For the banking information, a written request must be sent to all banks. This appears to constitute a challenge for the LEA both in terms of timeliness and in terms of analytical capacities as the data are not easily manageable.

[31] Total number of UTRs is of 19,520

Table 11: LEA information requests to FIU[32]

Year			2013	2014	2015	2016	2017	2018	6/2019	All years
Regional Headquarters of the Police Force		**operational section**	0	4	1	4	0	1	3	**13**
		investigating section	0	5	1	2	2	5	1	**16**
District Headquarters of the Police Force		**operational section**	1	6	13	1	3	2	2	**28**
		investigating section	6	6	4	5	6	6	2	**35**
The Bureau of International Police Cooperation[33]		**National Unit of Interpol**	8	26	43	69	49	38	25	**258**
		National Unit of Europol	3	20	18	41	60	48	34	**224**
The National Criminal Agency	**the Unit of the Financial Police**	**operational section**	29	18	15	21	14	15	7	**119**
		investigating section	1	0	0	2	1	1	0	**5**
	the Anti-corruption Unit	**operational section**	5	2	2	0	0	2	2	**13**
		investigating section	0	0	0	2	1	1	0	**4**
	the Anti-drug Unit	**operational section**	2	2	0	2	1	4	0	**11**
		investigating section	0	0	0	1	0	0	0	**1**
	the Anti-organized crime Unit	**operational section**	5	1	1	1	0	0	1	**9**
		investigating section	2	0	0	1	1	0	0	**4**
	the Department of the Fight against Terrorism / the National Anti-terrorism Unit		3	0	1	1	2	7	4	**18**
The National Criminal Agency (in total)		**Total**	**57**	**28**	**28**	**45**	**28**	**47**	**22**	**255**
		operational section	41	23	18	24	15	21	10	**152**
		investigating section	3	0	0	6	3	2	0	**14**

[32] No information was provided for the first 6 months of 2019.

[33] Requests sent directly to the FIU.

The Bureau of the Criminal Police		0	1	10	1	1	1	2	**16**
The Bureau of Inspection Service		2	0	0	0	0	0	4	**6**
The General Prosecutor Office of the Slovak Republic		2	2	0	3	0	0	1	**8**
Financial Directorate of the Slovak Republic		0	0	2	0	0	0	0	**2**
The Bureau of the Police Attaché		0	1	0	0	0	0	0	**1**
the Criminal Bureau of the Financial Administration	**operational section**	3	0	0	4	8	1	0	**16**
	investigating section	0	0	0	1	0	0	0	**1**
Total		**82**	**100**	**120**	**176**	**157**	**149**	**120**	**904**

145. The FIU can demand the postponement of transactions at the request of LEA or at the request from the foreign FIU. In case of an international cooperation request, if the transaction is not clearly identified, the FIU will ask the bank to postpone the first transaction of the client from a certain moment in time. Apart from international cooperation there are no indication of particular results in terms of ML/TF investigations obtained following the postponement procedures.

Table 12: Postponements requested by the FIU

Year	Number of postponements
2013	72
2014	141
2015	112
2016	196
2017	123
2018	71
2019	63

3.2.3. Operational needs supported by FIU analysis and dissemination

(a) Operational analysis

146. The operational analysis is performed within the FIU on the basis of the Order of the Director of the FIU on *"The Method of implementation of some provisions of the AML/CFT Act"* from 2018 (hereafter The FIU Methodological Order). The FIU Methodological Order lay down a UTR prioritisation mechanism (into three categories depending on the risk), and the steps to be taken in conducting financial analysis.

147. The first analytical stage after the receipt of the UTRs, consists of checks performed in the DMS to establish if the person (being natural or legal) is already there registered. The result goes to the Head of the UTR Department who decides to include the UTRs in one of the three categories A, B or C, depending on the case features.

148. The A category represents UTRs with high degree of risk, where immediate action at FIU level is required. Such cases would include on-going or terminated criminal procedures, risk for the funds to be transferred abroad, TF elements, or UTRs related to false ID or declarations by the customer etc. The B category represents an increased degree of risk, pertaining to complex and high volume of funds, disproportionate vis-a-vis customer's usual transactions; suspicions of EU funds frauds; funds related to state subsidies, public procurement, etc. The C category pertains to lower risk transactions where no immediate action from the FIU is required (such include refusals to execute a transaction or to establish a business relationship by credit institutions). According to FIU Methodological Order, the categories could be changed at any time if need be, but very rarely happened in practice.

149. The AT notes that the factors prioritising the UTRs are generally valid risks (such as postponed transactions or TF elements) but are not directly correlated with the actual country risks. For example, indicators that a PEP is part of the transaction will not lead to inclusion of the UTR in the A risk category.

150. The on-site discussions revealed that the percentage of UTRs categories go as follows: Category A – 10 %, Category B – 80 %, Category C – 10% which demonstrate that the system is not much of a help for the FIU analysis in concentrating their attention and focusing their resources, since as 90% of the UTRs go into a higher risk category.

151. Following the grouping in categories, the analytical process starts with NetReveal which adds to the case all the elements contained therein and generates a visualisation scheme. If additional information is needed, requests for information are sent to the obliged entities and/or additional searches are performed in relation to other linked natural and legal persons. International requests may be sent to foreign FIUs in this phase. Following the analysis, a report is prepared, with a proposal on the next steps to be taken: dissemination to LEA or archive for further use.

152. The analytical process is applied in the same way for TF related UTRs which are enriched with all available information and sent to the CTU-NAKA and SIS which in turn collect financial intelligence from FIs or through operative means (including surveillance). Unlike in ML cases, it appears that that FIU products are more widely used in TF operational phase in Slovakia.

153. The AT found that the FIU has at its disposal competent human capacities and actively uses appropriate analytical tools to produce results. Nevertheless, following successive restructuring, the number of FIU employees, the level of their salaries and their ranks remained the same. This situation makes the FIU less attractive for other Police employees and does not provide sufficient motivation for retaining the existing employees. In addition, the re-structuring was not considering the emerging needs of the FIU in terms of potential additional staff needed.

154. The weak outcomes in terms of support provided to the operational needs of competent authorities derive from the above shortcomings doubled by the lack of coherent management at the FIU level to gear their activities into becoming more effective.

(b) Strategic analysis

155. As mentioned in the TC Annex, the FIU should develop strategic analysis on new phenomena of crime related to ML and TF. However, in practice the FIU does strategic analysis only in the context of the annual reports. The AT had access to two such annual reports (for 2016 and 2017) and the analysis there included is commendable. Nevertheless, limited efforts have been

made to raise awareness of LEA on the findings of the annual reports with a view to use the conclusion in their activity. The FIU annual reports are not used strategically by LEA.

(c) Dissemination

156. FIU has full powers to disseminate the results of its activity to the competent authorities. Disseminations are made according to four separate provisions of the AML/CFT Act. Due to the convoluted dissemination system, the AT needs to re-iterate the provisions of the AML/CFT Act attaching explanations on how each provision is translated in practice:

i) Art. 26 (2) (b) of the AML/CFT Act is used when there is sufficient level of suspicion/indicators that ML or a predicate offence has been committed, in which case the file is submitted to the relevant LEA. These reports constitute the *"high level of suspicion"* ones and are to be found in Table 13 below.

ii) Art. 26 (2) (l) of the AML/CFT Act is used in cases of low level of suspicion/indicators which are used by LEA for further action.

iii) Art. 26 (2) (j) of the AML/CFT Act is used to inform the government authorities in the area of taxes, fees and customs. A big number of UTRs are disseminated according to this article to Financial Directorate of Slovak Republic (FDSR) and to a much lesser extent to FACO (see Table 14 below);

iv) under Art. 26 (3) of AML/CFT Act, the wording is vague[34] making it impossible to clearly distinguish who the recipient is, but the authorities interpret this as relevant for the UTR indicating higher security risk, including possible TF. In this case the file is disseminated to SIS and CTU-NAKA, and exceptionally to the Military Intelligence.

157. While technically compliant with the FATF requirements, the dissemination mechanism is puzzling and somehow deviates FIU's focus from the most relevant ML cases with a negative impact on effectiveness. In fact, a high number of UTRs are sent to LEA for *"further action"* which, translated into FIU work, represents a low level of ML indicators. Same goes for the disseminations made according to Art. 26 (2) (j) of the AML/CFT Act which are tax related. The result is that LEA do not take the FIU products seriously for prompt AML action, but mainly use them (if at all) in investigating other crimes. This opinion is confirmed by the fact that only two ML conviction have been achieved (in 2014) based on FIU disseminations, while 22 others have been used in convictions for other crimes.

158. The disseminations made according to Art. 26 (3) of AML/CFT Act are an area for concern as the wording of the sub-paragraph lacks precision and opens the door for various interpretations. It remains unclear for the AT which specific state bodies are authorised to receive FIU reports according to it, and in which circumstances, apart from SIS in case of TF suspicions. The authorities had difficulties explaining which practical situation would trigger such disseminations. There is no methodological instruction or written procedure to regulate the issue, especially with regard to the scope of disseminated information and the recipient authorities. For these reasons the AT is of the opinion that the said article constitutes a potential threat to the FIU operational independence and may jeopardise the safekeeping of confidentiality requirements.

---

34 "FIU provides all the information and documentation it has received under that law to the State authorities which carry out tasks in the field of protection of the constitutional system…"

CASE BOX 1: Conviction achieved based on FIU dissemination

In June 2014 the FIU received an UTR from a commercial bank with suspicions of ML linked to a foreign bank request to return allegedly fraudulently obtained funds. The owners of the account were two Cameroon citizen who, two days before the UTR received money from abroad followed by cash withdrawals in Slovakia and one internet banking transfer in a third jurisdiction. All those facts were included in the UTR.

The FIU requested the postponement for three days of any transaction that might have been ordered by the account owners. The amount of EUR123 342 has been frozen. In the meantime, all the checks were performed in the FIU DB, with no substantive outcome as no previous records on the two Cameroon citizens were available. The results of the DB searches together with the postponement decision were disseminated to the competent regional police authority. The LEA immediately issued a seizure order for the funds.

The FIU made an international information request in the jurisdiction of residence of the foreign bank. In less than 2 weeks the response from the foreign FIU was received and immediately submitted to the LEA.

In July 2014 the same bank sent a follow-up UTR containing the same ML scheme, this time related to an Egyptian citizen. This information was also disseminated by the FIU to the same LEA.

After examining the documents received from the FIU the Regional Prosecutors' Office started the criminal proceedings for money laundering. The predicate was found to be fraud committed against a company in Ukraine, with the money sent to a bank in SR and used as described above. In the context of the criminal proceedings three requests for mutual legal assistance (HU, TUR and NL) were issued (average execution time of 8 months). Finally, in 2017, two persons were convicted for ML with a penalty of 5 years imprisonment and 2 deportations were imposed.

159. In the period under review, the FIU has forwarded between 205 and 500 reports to NAKA Units, each dissemination including one or more UTRs. Turning to the district and regional Police units, they were the recipients of 2 486 UTRs based disseminations. Nevertheless, it seems that the latter very rarely (if ever) work on ML investigations or deal with the financial side of crimes. The AT was not informed of any success achieved in this regard.

160. Between 2013 and 2018, a total of 464 UTRs have been sent to the CTU – NAKA and SIS after being enriched with the available additional information the FIU disposes of. This represents 80% of the total number of the TF UTRs received by the FIU. Within both SIS and the CTU – NAKA all the TF related UTRs undergo checks and, depending on their nature and initial assessment, further steps are taken. One criminal investigation was launched based on FIU disseminations, all the rest of cases being ended at operational level. According to the CTU – NAKA and SIS, the FIU reports contribute to an operational work related to persons suspected of TF or complete ongoing inquiries of suspected persons/entities.

161. Despite a relatively high number of TF FIU disseminations, the majority of suspicions were based only on the refusal of the bank to open an account for persons with ties with high risk countries/regions or on transactions linked with such country. Partial matches with Worldcheck lists (not UNSCRs) were sometimes reported. Only a small part of the UTRs met the attributes of substantial TF suspicions.

Table 13: Investigations based of FIU disseminations to LEA[35]

Year	UTRs	Disseminations	Money Laundering (Art.233)			Other crimes		
			Prosecution	Indictment	Conviction	Prosecution	Indictment	Conviction
2013	3 886	267	7	1	0	27	1	4
2014	3 928	406	65	2	2	67	13	7
2015	3 264	333	23	4	0	31	10	10
2016	3 297	498	31	1	0	33	1	0
2017	2 636	354	53	3	0	28	1	1
2018	2,509	252	34	1	0	17	5	0

162. The Slovak authorities keep different types of statistics when it comes to disseminations. As described above, the higher degree of ML suspicions is born by the disseminations made according to Art. 26(2)(b) of the AML/CFT Act (see Table 13 above). Nevertheless, there are other disseminations made in accordance with Art. 26(2)(l) and (j) and Art. 26(3) of the AML/CFT Act, for which separate statistics are not available. All disseminations (including those made under Art. 26(2)(b)) are displayed in the Table 14 below.

Table 14: UTRs based disseminations[36]:

Authority/year	2013	2014	2015*	2016*	2017	2018	Total
National Criminal Agency of the Police Force Presidium	540	328	256	281	223	295	1,923
Anti-Terrorist Unit	80	79	83	93	69	60	464
Unit of the Financial Police	419	230	157	174	138	205	1,323
Anti-Corruption Unit	1	0	0	4	2	6	13
Anti-Drug Unit	8	2	0	3	4	15	32
Anti-Organized Crime Unit	26	14	9	4	2	7	62
Asset Recovery Office	3	1	2	1	0	0	7
Obliged Entities´ Control Department of FIU	3	2	5	2	8	2	22
District and Regional Headquarters of the Police Force	321	488	378	567	419	313	2,486
District Headquarters of the Police Force	309	431	333	489	369	283	2,214
Regional Headquarters of the Police Force	12	57	45	78	50	30	272
Other							
Financial Directorate of the Slovak Republic (FDSR)	1 636	1 551	1 391	1 361	1 138	980	8 057
Bureau and/or Directorate of the Border and Foreigners Police of the Police Force Presidium	0	0	2	4	0	3	9

[35] Disseminations made only according to para 26 (2)(b) of the AML/CFT Act (suspicion/criminal behaviour is better described, and a possible crime is identified)

[36] All disseminations by FIU.

Section of Control and Inspection Service of the Ministry of Interior of the Slovak Republic	4	1	0	0	3	1	9
Criminal Bureau of the Financial Administration (FACO)	27	11	11	8	6	12	75
Bureau of the Criminal Police of the Police Force Presidium	0	3	1	0	2	1	7
Bureau of International Police Cooperation of the Police Force Presidium (Interpol, Europol, Sirene)	0	0	2	4	0	4	9

** - total number of information forwarded to the National Criminal Agency differs from information contained in annual report, because annual reports do not include the Anti-Terrorist Unit of the Police Force Presidium, Asset Recovery Office and the Obliged Entities´ Control Department of FIU*

163. The FDSR has received most of the FIU's disseminations (8 057 UTRs), representing more than 40% of UTR (see Table 14 above). The information obtained from the FIU has a significant impact on the risk profiles of the tax-payers, legal entities, on the basis of which they are subsequently selected for tax audits or local surveys (see Table 15). Without prejudice to the results obtained in fiscal/taxation area, the AT must note that those remain limited to tax audits (which are outside the core functions of an FIU as required by IO6).

Table 15: FIU information used for tax audits purposes

Year	Number of information received from FIU	Number of open tax audits for entities revealed from information received from FIU	The rate of FIU information that has affected the risk profile of an entity when opening a tax audit
2014	1 432	777	54,26%
2015	1 370	740	54,01%
2016	1 255	691	55,06%
2017	1 097	555	50,59%
2018	927	419	45,20%
TOTAL	**6 081**	**3 182**	**52,33%**

164. Only a marginal number of the FIU disseminations to FDSR is actually sent to FACO, which is the law enforcement arm of the FDSR (see also the analysis under IO7). The authorities maintain (and the AT has no reason to disbelieve) that, as part of specialized tripartite teams "Tax Cobra" (Tax Specialist, Investigator of Police Force, Supervision Prosecutor) the FDSR uses the information from FIU (financial transactions of corporate entities, information about the shell companies run by the so-called *"white horses"*) to investigate serious tax crime. Less results have been reported on ML investigations with proceeds resulted from tax crimes which would have added to the effective support provided by the FIU to the operational needs of the competent authorities.

165. The Slovak authorities claim that in practice, when conducting tax audits, the FDSR does not reveal or inform the subject about the previous FIU dissemination. Nevertheless, it is unclear if the confidentiality requirements are observed in all cases, and how is the potential risk of tipping off addressed. The AT was not provided with any risk assessment or mitigation measures taken in this area.

166. The quality of FIU disseminations is uneven, with most of the representatives of the LEAs considering the quality of the FIU reports insufficient to trigger a ML investigation, or to be otherwise effectively used in a financial investigation. In some instances, the FIU information is used for investigations into other crimes.

167. Having said that, this statement needs to be nuanced as the LEA demonstrated a very limited appetite in investigating ML cases and in conducting financial investigations in general. Only the Financial Police Unit NAKA and Anti-Crime Unit NAKA are satisfied that the UTR's based disseminations are qualitative this being translated in a higher number of ML cases, although no statistics were available in this regard. By the rest of the LEA, the FIU is mostly considered as a tool to obtain the data on the accounts abroad, trough Egmont GROUP or other FIU channels. In other words, the quality of the FIU disseminations is an area for improvement, but the disseminations could still be used to support the operational needs of LEA, provided that they are willing and ready to engage in financial investigations.

3.2.4. Cooperation and exchange of information/financial intelligence

168. There are no impediments, statutory or otherwise, which hinder the domestic and international exchange of financial intelligence. The FIU is able to share information with domestic LEA (through disseminations and case-by-case requests) and foreign FIUs. Where information is needed formally (either from or by the FIU), a written request is submitted (see Table 11 above). Law enforcement authorities exchange information both domestically and internationally based on the Act on Police Forces, the Act on SIS, as well as on the basis of EU framework.

169. The AT was satisfied that all competent authorities, including LEA and financial supervisors, are willing to share information with the FIU and do so when so requested. The FIU has broad access to governmental databases. Informal information exchange does not appear to be a common practice in Slovakia.

170. The FIU provides law enforcement authorities with financial information both spontaneously and upon request, and, when necessary, the law enforcement authorities seek additional information about BO and source of funds when needs to be obtained from foreign counterparts. As stated above, the financial information provided by the FIU to domestic LEA is limited to DMS. The FIU's assistance is requested by LEA when there is a need to obtain information about bank accounts outside Slovakia, trough Egmont GROUP or other FIU channels. FIU collects the same type of intelligence on behalf of foreign FIUs as in case of their own analysis.

171. While disseminating, the FIU has the authority to decide to which NAKA or district/regional PF unit will forward UTRs based disseminations. There is no single-entry point in NAKA or elsewhere in PF which would receive and assess who should be recipient or recipients, with possible coordinative action. According to authorities, in the past there were cases where two different units were investigating the same persons/criminal activity. AT is of opinion that NAKA and other PF units need higher level of cooperation and coordination regarding receiving, obtaining, analysing and use of financial intelligence.

172. FDSR has a good cooperation with NAKA in sharing information from their databases and providing valuable support, for example through analysis prepared using the analyst notebook. The requests to FDSR are individual, not as part of a formal mechanism and the number of cases were such cooperation and information exchange is carried out is up to 10 per year.

173. SIS performs summaries and analyses which are then sent to PF in the form of information for further investigation either upon request or spontaneously. The cooperation with the FIU was

reported as satisfactory.

174. At the international level the FIU appears to be active and responsive (see Table 58 under IO2). There are no requests from foreign counterparts which remained un-answered and the feedback provided by the international community regarding the Slovak FIU was generally positive.

175. Between LEAs, the information exchange remains an area for improvement. While there are no ML specialised units, little financial intelligence is exchanged horizontally. With the new NAKA organisational scheme, it is expected that ARO shall provide financial profiles to other police units when required, but due to recent implementation of the change, this could not be confirmed by the AT.

176. The Police Force co-operates with the police of other states, with international police organisations, international organisations and organisations operating on the territories of other states, primarily by exchanging information (including financial intelligence), exchanging liaison officers, and other possible forms.

177. NSAC platform under SIS supports the exchange of financial intelligence, especially regarding TF matters. Representatives of SIS and number of other authorities met on-site mentioned NSAC as a tool which enhance cooperation and coordination. Although there were no concrete examples of cooperation regarding exchange and use of financial intelligence, it can be pointed out that NSAC is more relevant for FT cases.

178. Communication and coordination through feedback on ML cases remains insufficient. Feedback on the use of financial intelligence from the LEA to the FIU and from Prosecution to LEA is insufficient to contribute to improving the quality of analytical/investigative products. Improving this system would benefit to the entire upstream information chain up to the REs.

Overall conclusions on IO.6

179. There are no impediments encountered by FIU and LEA in accessing financial intelligence and other information to develop analytical products. However, the use of the financial intelligence by LEA is modest. The FIU receives most of the UTRs through encrypted e-mail communication and store them subsequently in a self-developed DMS. The number of UTRs received is relatively stable and reasonable. While the information contained therein is current, there are concerns on the quality of the suspicious. The FIU has at its disposal sufficient human capacities and actively uses appropriate analytical tools to produce results. The weak outcomes in terms of support provided to the operational needs of competent authorities derive mainly from questionable dissemination system and lack of coherent management. The AT is satisfied that all competent authorities, including LEA and financial supervisors are willing to share information with the FIU and do so when so requested.

180. **Slovakia is rated as having a Moderate level of effectiveness for IO.6.**

3.3. Immediate Outcome 7 (ML investigation and prosecution)

181. The legal framework for the criminalization of ML has not significantly changed since the previous round of evaluation, apart from an amendment by which the scope of the ML offence in Art. 233 CC was extended to proceeds of criminal activity (instead of a criminal offence) hence demonstrating the inclusive character of the offence.

3.3.1. ML identification and investigation

182. Since the 4th round of evaluations, the Slovak Republic slightly improved its legal and institutional frameworks pertaining to ML investigations. At the inception of the criminal phase, the number of cases increased twice (369/829) as well as the number of persons accused (195/421). The indictments increased three times (72/244), while the final convicted persons increased to a lesser extent. (58/94).

Table 16: Dynamic of ML investigations and prosecutions since the previous round of evaluations

	4rd	**5rd**
Commencement of ML criminal proceedings	369	829
Persons accused	195	421
Persons indicted (pending in Courts)	72	244
Persons convicted	58	94

183. The investigations in Slovakia consist of several stages. The first is the pre-investigative phase, which falls under the competence of the (operational) police forces and the FACO. This is the entry gate for most of the ML cases including some of the FIU disseminations, and comprises searches, analysis of financial information etc…

184. In the pre-investigative (operational) stage, in the process of search for property and elaboration of a property profiles, information on bank accounts and on movable and immovable assets is analysed in accordance with the Act on the Police Force. Practitioners interviewed on-site maintained that this type of information is not always accepted as evidence and it is of informative nature for the investigators. Nevertheless, the practice is in train of being unified as on 23 September 2019, the Criminal Law College of the Supreme Court issued an opinion which allows the possibility for measures instituted before prosecution to be used as evidence in criminal proceedings.

185. If following the operational activities, the case is strong enough, it is sent to the investigator, who initiates a formal criminal investigation under Art. 199/1 CCP, or under Art. 206/1 CCP if the perpetrator is known and he/she shall be charged. If the necessary information does not prove the case in the pre-investigative phase, the matter is terminated at the operational level.

186. While the legal framework corresponding to the criminal investigation phase appears to be adequate to the threats, the assessors have concerns regarding the operational stage, where there is a lack of timeliness and adequate monitoring to evaluate the manner in which, globally, the police handles the ML cases effectively in the application on *"follow the money"* principle.

187. There is no dedicated LEA to investigate ML offences which, as a matter of principle, are dealt with by the authority having competence over the predicate offence. Legally, financial investigations should be carried out based on the general authorization provided by Art. 119 (1) (d) and (f) CCP, in all criminal cases related to proceeds generating offences and particularly in those which would potentially include property forfeiture as an obligatory punishment (Art. 58 (2)(3) CC).

188. At the methodological level there are two main documents intended to assist police officers and prosecutors in handling financial investigations: the *"Recommendations on financial investigations for all district and regional prosecutors"* approved by the GPO in May 2017 and the *"Methodical Guidance"* issued by the Presidium of the Police Force in January 2017. To those, other

documents were issued with less impact on effectiveness[37]. In practice, financial investigations are not routinely done, the application of such depending on the specific LEAs and the circumstances of the case.

189. Throughout the board, there are no specialised police officers in handling ML cases and the awareness and knowledge on the how to deal pro-actively with parallel financial investigations is un-even and generally insufficient. Nevertheless, there are some differences between various Police Forces and FACO in their ability and readiness to venture into a ML case. While the Financial Police Unit NAKA and the ARO NAKA are keener to start or support a ML investigation, others openly admit having significant challenges in doing so.

Table 17: Number of ML investigations initiated by all LEA

ML investigation in operational stage		Commencement of criminal proceedings (cases)	Persons accused	Terminated Criminal Prosecution (cases)	Indictment/persons	Convictions (cases/persons)
2013	62	103	82	128	35	8/11
2014	62	113	63	118	36	8/12
2015	56	125	34	158	56	6/9
2016	60	130	32	118	39	11/23
2017	61	209	94	110	58	15/22
2018	65	149	116	93	20	6/10
06.2019	N/A	40	24	14	4	4/7
Total	**366**	869	**419**	**739**	**248**	**58/94**

190. In the period under review, 366 ML investigations have been started at operative level which number increased at 829 at the beginning of the criminal proceedings and ended up with 84 final convictions. The rise in the number of investigated persons after the beginning of the criminal procedures is mainly due to: i) rather superficial financial analysis at early investigative stages and ii) the extension on the case (persons, transactions, criminal acts retained) at prosecution stage.

191. At the various Police Forces (see the sub-chapters below), ML statistics are not kept, hence the AT did not have at its disposal more detailed information on investigations carried out by specific Police body, apart from the sporadic and un-structured data provided individually.

192. Although generally the police officers have the statutory competences and some guidance into conducting financial investigations, the effective investigation of ML cases in terms of number and profile remains limited. The assessors note that LEAs is more effective in collecting information on predicate crimes but do not appear to pay due attention to the identification of

[37] March 2015 - GPO/Analysis of the limits Assessment of effectiveness in the activity of the General Prosecutor´s Office in the field of criminal prosecution of money laundering and seizure of proceeds of crime with regards to MONEYVAL standards and recommendations; December 2015 - Measure no. 39 from the meeting of the General Prosecutor from 9 – 11 December 2015– updated 12 September 2018 – setting up obligation/framework of performance; January 2017 "Methodological tool of financial investigation"; 30.09.2017 Evaluation of the performance of so-called financial investigation in criminal matters for which the Criminal Code sets out the punishment of forfeiture of property as an obligatory punishment for the period 2015 – 2016 and related "Recommendations on financial investigations for all district and regional prosecutors"; 03.06.2019 - Measure of the General Prosecutor's office of the Slovak Republic, implementing the national risk assessment on money laundering and the financing of terrorism under the conditions of the Slovak Republic for the period 2011-2015; Strategic principles in the fight against money laundering, the financing of terrorism and financing of the proliferation of weapons of mass destruction for the period 2019 – 2024; Action Plan of the fight against money laundering and the financing of terrorism for the period 2019 – 2022; and Recommendation no. 6 of the evaluation report on the eighth round of mutual evaluations "The practical implementation and operation of European policies on preventing and combating environmental crime" – Slovak Republic, under the conditions of public prosecutor's offices.

proceeds and to associated ML activities. Even when financial investigations are carried out, they are mostly geared towards identifying the location of the proceeds with a view to applying provisional measures rather than initiating a potential ML case.

193. At strategic level, the AT was not convinced that ML is prioritised by other LEAs as an offence worth pursuing in its own right as long as the predicate crime is investigated, and the related proceeds are seized. The assessors noted some deficiencies in the cooperation and coordination between the law enforcement and prosecutorial authorities throughout the life cycle of a ML case which prevents authorities to act faster and more effectively. An example of such is the limited monitoring at the pre-investigative phase and the lack of mechanism to avoid duplications. Consequently, various opportunities to identify ML cases in the course of an investigation of a predicate crime appear to be missed.

194. Another significant challenge the Slovakian system encounters is the abnormally lengthy procedures to achieve a ML conviction, especially if we consider the moment of the crime and the moment of the final decision of the Court. This appears to be generated by several factors which have been analyzed throughout IO7 but it is mainly due to lack of specialization in dealing with the financial side of crimes and absence of opinions and precedents by the Supreme Court which would unify the practice.

National Financial Police Unit of the NAKA (hereafter Financial Police Unit NAKA)

195. In practice, the Financial Police Unit NAKA deals with most ML offences. This is generated by three factors: first, Financial Police Unit NAKA is in charge with criminal offences of economic nature and ML is considered as one; secondly, most of the ML cases have economic crimes as predicates; and third, the Financial Police is NAKA's main LEA recipient of the FIU disseminations (see tables under IO6).

196. There are several avenues for starting a ML case: i) Disseminations received from the FIU; ii) notifications based on operative and intelligence activities (including investigations into the predicate offence); and iii) upon receipt of complaints from the damaged party.

197. The statistics broken down by LEA recipient kept by the FIU demonstrate that in the period 2013-2018 a total of 1 025 notifications were sent to the Financial Police Unit NAKA which in turn initiated only 27 ML investigations. These 27 investigations comprise all potential sources that would trigger a case and the AT was not provided with more detailed statistics. In any event, the output in terms of ML investigations is low if compared with the input received from the FIU. To prove the existence of cases initiated by FIU disseminations the authorities provided the case below.

CASE BOX 2: The "Facebook case"

Predicate offence: Fraud. The perpetrator misled the representatives of the securities brokerage company by changing the contact details and bank account number of the client of the company, on behalf of the client, ordered the sale of the Facebook share, which was realized, causing him a damage of EUR 78 683.

ML element: The owner and the executive officer of the company M - received funds, which were credited on the bank account of the abovementioned company for a fraudulent sale of Facebook shares owned by P. V. and managed by the company at the amount of EUR 78 683.

Identification of the case (relevance to IO 2 and IO 7): This case was initiated on the basis of FIU dissemination dated 20.10.2016 in which case we can point out the cooperation of financial

police with FIU when the money was postponed in the account pursuant to AML Act before the seized money pursuant to §95 of the Criminal Procedure Code. During the criminal investigation actions of a covert nature were performed, witnesses were questioned, financial investigations were conducted and seizures and examinations of items were carried out.

Property seizure and freezing (relevance to IO 8): Assets were seized during the pre-trial investigation, including bank accounts. In accordance with § 95, funds were seized in full on the accused's account EUR 78 683.

Status of the case: In 2019, the District Court of Bratislava convicted one person of ML and fraud, with a sentence was 3 years of imprisonment.

198. Financial police investigators are obliged to identify the proceeds of crime and apply provisional measures. The Financial Police Unit NAKA officers are moderately aware of the specificities of the financial investigations in ML cases (*i.e.* that might be committed by persons with knowledge in the fields of economics, law, tax, customs as well as use of *"straw men"* in case of legal entities etc…), but they still lack a more structured and deep professional knowledge, skills and resources to effectively carry out financial analysis and investigations in proceeds generating crimes.

199. In order to find and seize evidence, the police officers are entitled to apply the usual investigative measures such as personal and premises searches, seizure of PC data and other devices. In criminal proceedings, bank information is obtained upon a written request sent with the prior consent of the prosecutor. In the absence of a bank account register (see also analysis under IO5), the police officers shall address the request to all banks or branches of foreign banks operating in the SR.

200. In pre-investigation phase, the operative employees of the Financial Police Unit NAKA are entitled to request information from the FIU, but in case of banks, the 30 days delay remains. The information so obtained cannot be used in the criminal procedure but only for intelligence purposes.

201. There are no specialized investigators within Financial Police Unit NAKA to deal with ML cases. This situation creates significant difficulties not only for them, but in a *"cascading effect"*, for all other Police Forces which informally consider the Financial Police Unit NAKA as the *"ML and financial investigations specialised body"* which would provide specialised analysis and/or take over the case into a ML investigation.

202. Although the police officers have the statutory competences and some guidance into conducting financial investigations, the AT has concerns on their practical application as: i) the Financial Police Unit NAKA does not have sufficient resources (*i.e.* timely access to information including DB, trained personnel, analytical tools etc...) to conduct financial investigations into ML and proceeds generating cases and ii) other Police Units do not have sufficient knowledge and awareness on the importance of financial investigations to address requests to Financial Police Unit NAKA at least in serious proceeds generating criminal cases under their competence.

Property Investigation Department – NAKA (Hereafter ARO NAKA)

203. The ARO – NAKA has been created in February 2017 as a sub-unit within the Financial Police Unit NAKA (before that, ARO was part of the FIU), therefore contributing to the financial investigations on ML and proceeds generating crimes as described above. ARO – NAKA has the role of the Slovak Asset Recovery Office pursuant to the *"Internal regulations of the national criminal*

agency of the Presidium of the police force" from 2017, and EU legislation.

204. Since 1 October 2019, ARO – NAKA has been re-allocated to the department of Analysis and Supporting Activities of NAKA with the purpose to provide support for all LEA, both in operational and criminal procedure stages.

205. In terms of financial investigations, the core-function of the ARO – NAKA is to prepare a *"property profile"* (or *"assets profile"*) of natural persons or legal entities which are subject to financial investigations. In the process of search for property and creation of a property profile, operational information on bank accounts, movable and immovable assets is ascertained. The property profiles and the information about the assets are the basis for producing evidence in criminal proceedings, in order to seize or confiscate the property.

206. Turning to financial investigations beyond the *"property profile"*, ARO's assistance is not automatically available for all LEAs, but only if there is an international aspect, or on a case-by-case basis, subject to the decision of the director of the NAKA. The AT was not convinced that the ARO – NAKA has sufficient knowledge and capacities to pro-actively contribute to potential ML cases.

207. The AT took note of the re-localisation of ARO – NAKA outside the Financial Police Unit NAKA and the potential benefits for the production of meaningful financial analysis for ML and proceeds generating cases. Nevertheless, since this change occurred just days before the on-site visit, no further credit can be given to this unit in the context of IO7.

Anti - Corruption Unit NAKA, Anti-Crime Unit NAKA, Anti-Drug Unit NAKA and the National Unit Combating Illegal Migration of the Bureau of Border and Foreign Police of the PF Presidium (Hereafter Anti - Human Trafficking Unit)

208. The three NAKA Units and the Anti- Human Trafficking Unit are analysed together as there are no major differences in the manner of identifying and investigating potential ML cases were observed.

209. The same avenues for starting a ML investigation apply, as in the case of the Financial Police Unit NAKA (see above). The significant deviation is that the other NAKA Units and the Anti-Human Trafficking Unit are receiving much less FIU disseminations then the Financial Police Unit NAKA (see Table 14).

210. The financial investigations should be carried out whenever the circumstances of the case indicate that ML has been or is occurring. In practice, financial investigations are performed to a limited extend and are almost exclusively aimed at identifying and tracing the proceeds from the criminal activity for seizure and confiscation purposes rather than to identify and start a potential ML case.

211. The representatives of these police units consider ML as very difficult crime to prove seeking very complex forms of laundering, as they do not appear to have absorbed sufficient awareness about all forms of ML, especially simpler ones (*e.g.* where a fake contract or a false declaration is not present). *"Simple"* ML cases are mistakenly considered as mere consumption of proceeds and are not pursued. Some on-going investigations demonstrate that pursuing ML without a clear link to the predicate crime is possible (see case box below). Nevertheless, not all police officers agree with this view as during the interviews some stated that a direct link between the funds and the predicate crime is expected to be established.

CASE BOX 3: The SITINA CASE

Predicate offence: On 27 November 2019 two persons from the highest controlling and managing bodies of the Company T. were accused of exceptionally serious criminal offence of Violations of Obligations of Trust pursuant to Section 237(1)(4)(a) of the CC and of ML. The accused in the period from 2012 until 2018, despite obtained knowledge about the abuse of the gaming system, contrary to its rules, intentionally failed to take effective measures to prevent the abuse of monetary deposits to individual gamer accounts deposited by means of anonymous bank cards Paysafe Card and CardPay in larger volume and with smaller nominal values, what lead to subsequent payment of such deposits from gamer accounts of registered gamers to various others, as yet unidentified bank accounts in the country or abroad without actual gaming with products of the internet gaming system eTipos, whereas they thus allowed in min. 142 cases to perform uncontrolled transfer of finances with regard to anonymous deposits and subsequent withdrawals in the amount min. EUR27 000 000, thus acting contrary to the obligation to notify and report unusual trade transaction.

ML element: Abuse of the cash deposit system for individual player accounts deposited through anonymous Paysafe Card and CardPay bank cards.

Identification of the case (relevance IO 7): The case was identified by the Anti-Crime Unit NAKA in detecting organized crime activities in the field of money laundering. During the investigation, several employees of the lottery company were heard and the accounting documents and data repositories were seized. At the same time, a financial investigation is conducted and at least 143 bank accounts are being analysed. Average value of funds on detected bank accounts - EUR27 000 000.

Property seizure and freezing (relevance to IO 8): Preparations are underway to secure the proceeds of crime and arrest the perpetrators.

Status of the case: The case is still under investigation and is supervised by prosecutor of ÚŠP. The case demonstrates the ability to prosecute ML without a clearly defined predicate criminal activity.

212. The NAKA units are not able to effectively identify potential ML cases, or to conduct financial investigations more generally, as they do not have specialised analytical staff. To conduct financial investigations or analysis, they are dependent on the ARO and Financial Police Unit NAKA. In turn, due to resources constraints, the Financial Police Unit NAKA would undertake a financial investigation to support another unit only if there is proof of significant amounts involved. In AT's opinion this is a too high requirement and it dissuades the pursuit of all ML cases.

213. The above conclusion is confirmed by the actual results achieved by the NAKA units in relation to ML investigations. While the Anti-Crime Unit NAKA and the Anti - Corruption NAKA reported five, respectively one ML investigations (see CASE BOX 3 and 4), the other two have no experience in this respect.

CASE BOX 4: "THE APPLICANT" case

Predicate offence: Thirteen natural persons and five legal persons forming an organized group to commit -active corruption and trading of influence**.**

Factual basis and ML element: The accused in 2018 in Bratislava and other places in the territory of the Slovak Republic joined to purpose of committing corruption offenses by receiving bribes and indirect corruption on the Bratislava District Office, in particular in the form of false mandate

contracts concluded pursuant to § 566 of the Commercial Code.

Identification of the case (relevance to IO7): As part of the investigation into corruption crime, it was found that the perpetrators received bribes legalizing in the form of mandate contracts for several companies that did not actually carry out any activities. During the FI was established evidence in relation to: Bank accounts, real estate register, commercial register, Social Insurance Agency.

Property seizure and freezing (relevance to IO 8): 1 bank accounts secured through Art. 95 CCP – the sums so far secured: EUR118 500**.** The cash secured during home searches: EUR40 000

Status of the case: ongoing investigation by **Anti-Corruption NAKA supervised by USP.**

The Criminal Office of the Financial Administration (FACO)

214. The FDSR is authorized to conduct administrative and criminal proceedings having powers in the area of fiscal discipline. Administrative–legal proceedings can be divided into customs proceedings and tax proceedings.

215. FACO is a special unit within the FDSR entitled to detect and investigate criminal offences in the area of customs and tax regulations. FACO agents execute their duties according to the CCP and investigate criminal offences committed in connection with the violation of customs and tax regulations.

216. A ML criminal prosecution can be conducted by FACO only in parallel with a predicate crime. A specific feature of these proceedings is that a competent authority is entitled to recover tax or customs evasions in administrative proceedings (tax and customs), which constitutes *"damage"* for the purposes of criminal proceedings.

CASE BOX 5: "THE NEPHEW"

The criminal acts (tax crimes) took place in 2013-2014, when OCG imported from Poland mineral oil, which was then sold in Slovakia as Diesel oil, using a scheme of fictitious suppliers and buyers and physically operated a "fake" petrol station which were, for example, agricultural cooperatives, which are not official gas stations, but also offer the possibility of fuelling to natural persons.

The damage to the state budget was estimated at EUR 23 314 516 (excise duties and VAT).

ML element: Two out of 22 persons accused were charged for ML in additional to the charges for the predicate crimes. The laundering consisted in using the proceeds to acquire real estates of a value of over EUR 1 000 000.

Identification of the case: The investigator initiated a criminal prosecution for the crime of tax and insurance evasion (on the 10th May 2013) which was extended to ML (on the 14th May 2015). In the context of the financial investigations, the following actions were taken:

- the joint financial investigation plan (FACO – NAKA – FIU) was signed by all parties and the property profiles of all accused individuals were drawn up. The bank accounts of the accused individuals and companies managed by them in six banks in total were identified and at least 50 bank accounts were analysed;

- information from the Geodesy, Cartography and Cadastre Authority related to the real estate seized in the criminal proceedings was obtained and analysed;

- requests to National Motorway Company, Social Insurance Agency, tax authorities and Customs authorities have been issued.

Mutual legal assistance was requested and provided by Poland, Hungary, Czech Republic, Bulgaria, Romania, USA.

Confiscation of proceeds and instrumentalities (relevance to IO 8):

200 000 litters of mineral oil, 12 tractors with tank semitrailers (instrumentalities), 5 cars (estimated value EUR 41 000), 5 real estate properties (estimated value: EUR 1 104 450), 20 computers and laptops, cash found during house searches (EUR 65 705).

Status of the case: In July 2017 the Specialised court convicted two persons for ML with cumulated sentences (ML plus predicate offences) of for 14 years, and 12 years. In March 2019 the Appeal court upheld the decision.

217. Depending on the amount of the damage and the possibility to recover it by the competent tax or customs authority, FACO investigators consider whether ML was committed following the instructions of the supervising prosecutors.

218. FACO receives a modest number of the FIU disseminations (see also Table 14) and achieved one ML conviction (see CASE BOX 5). The FIU took part in the investigation but the case was not triggered by an FIU dissemination.

Office of the Criminal Police of the Police Force Presidium (Hereafter Criminal Police)

219. The Criminal Police performs investigations based on territorial jurisdiction: the location where the ML was committed, where the suspected person is residing or where the legalization was revealed. Aside from the territorial jurisdiction, the main criterion for determination the subject-matter jurisdiction (Criminal Police Departments of the District Directorate, Criminal Police Departments of the Regional Directorate or the NAKA) is given by the extent of ML, respectively by the amount of proceeds obtained.

220. The Criminal Police both at District and regional level are important recipients of FIU disseminations. Nevertheless, they seem to favour the initiation of a ML case by operative work as in case of any other crime.

221. The financial investigations are performed according to the Methodological Guidance issued by the GPO, which the Criminal Police investigators commonly consider as being only a basic theoretical minimum which is insufficient to support the conduct of financial investigations.

222. Overall, the financial investigation is not separated from the *"standard"* investigation and it is carried out by an investigator who does not have special AML training. Within the time limits in which the investigation of the predicate offence must be completed, the Criminal Police investigators find it challenging to carry out a diligent and effective financial investigation, which is considered much more time-consuming to ensure the necessary evidence to prove the ML crime. A particular situation are the custodial cases which must be handled with priority and in a timelier manner.

CASE BOX 6: ML and cybercrime

On 24.07.2014 a commercial bank sent an STR to the Slovak FIU based on suspicions related to incoming funds from Ukraine in the account of a foreign natural person (Mr X), opened in Slovakia. The transaction was not executed and the FIU instituted the postponement of the transaction for 72 hours. In the course of the analysis the FIU identified another related bank account opened on the name of other foreign citizen Mr Y, put all the data together and informed Regional Criminal Police. The value of the frozen money was of EUR67 161. The same day the investigator contacted

the Prosecution and formally started the criminal proceedings. A Financial investigation was launched and a total of EUR123 342 (the entire sum exiting in the two identified bank accounts of Mr X) was seized by Prosecution.

The investigation indicated that the money was the result of cyber-frauds by which the Ukrainian company was instructed to redirect payments due to its business partners to the bank accounts of Mr X in Slovakia. The fraud was confirmed by the Ukrainian authorities through MLA but no conviction was pronounced in Ukraine before the ML conviction in Slovakia.

Mr X and Mr Y remain silent and based on circumstantial evidence the Court in Slovakia was convinced of the criminal origin of the funds and convicted them in 2017 for ML (5 years imprisonment and deportation for 15 years). The money was seized and returned to the damaged person's (Ukrainian company) bank account during the pre-trial proceedings.

Prosecution

223. The Prosecution service is structured into General Prosecutor´s Office, Regional Public Prosecutor's Offices (8) and District Public Prosecutor's Offices (54). The Special Prosecutor's Office has competences in matters falling within the jurisdiction of the Special Court, mostly related to corruption in a broader sense, offences damaging the financial interests of the European Union, organised crime and serious damage crimes (exceeding EUR6 650 000). The Regional Prosecutor's Office has territorial competences.

224. In practice, a ML case is taken over by Prosecution when the case is already investigated by the Police based on: i) Disseminations received from the FIU by the Police Units which have passed the operative stage ii) Notifications of the investigative body based on operative and intelligence activities (including investigations into the predicate offence) and iii) upon receipt of complaints from the injured party. In addition, the prosecutors may order or initiate prosecution or directly commence the criminal proceedings on the basis of an evaluation of its own information (*e.g.* from the media or from analyses of investigated cases…).

Table 18: ML cases by level of Prosecution and stages of criminal procedures.

ML cases – pre-trial proceedings – overview by particular level of prosecution offices								
Persons accused - § 206 CCP								
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**06.2019**	**Total**
CPO	46	31	18	19	19	105	12	**250**
RPO	20	17	9	8	6	7	2	**69**
GP/TO	3	0	0	0	0	0	0	**3**
ÚŠP	13	15	7	5	69	4	10	**123**
Total	82	63	34	32	94	116	24	**445**
ML cases - overview by particular level of prosecution offices All forms, by which the cases were finally terminated: an indictment, a conditional suspension, a settlement, an agreement on guilt and punishment **- persons –**								
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**06.2019**	**Total**
CPO	31	37	26	11	19	9	4	**137**
RPO	7	4	16	23	19	6	2	**77**
ÚŠP	5	5	23	16	30	7	6	**92**
Total	43	46	65	50	68	22	12	**306**

CPO – County Prosecution Office; GPO – General Prosecution Office (Criminal Department); RPO – Regional Prosecution Office; ÚŠP – Special Prosecution Office.

225. The assessors noted a significant increase in the number of ML indictments which is less visible in case of ML convictions. The gap between the number of indictments and convictions appears to be the unreasonable lengthy procedures, due to uncertainty as to the level and quality of evidence that would be needed to convince the judiciary of the subjective element, and that funds were derived from a certain crime. The judges continue to have a strict interpretation attributed to the ML offence as described below. Although statistics are not available, the authorities maintain that the number of cases returned by the Courts is not high. Another challenge is the apparent reluctance to pursue associated ML charges in case of simplified procedures (*i.e.* plea bargain) for the predicate crime, as well as the strict interpretation of the material elements of the offence such as the element of concealment.

226. There are no significant differences between different levels of prosecution offices, and they all appear to be involved in ML cases. Since 2015, concrete efforts have been made by prosecution to target ML as an offence worth pursuing in its own right, separately from the predicate crime. This is supported by a number of investigations presented to the AT, some of which have already resulted in ML convictions.

Table 19: ML cases by stage (2013-2019)

ML CASES – Prosecution – Convictions								
YEAR	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**30.06.2019**	**Total**
Commencement of criminal prosecution	103	113	125	130	209	149	40	869
Terminated Criminal Prosecution of Unknown perpetrators	128	118	158	118	110	93	14	739
Persons accused	82	63	34	32	94	90	24	419
Finalized criminal Prosecution of Accused Persons	61	632	73	81	75	36	12	400
women	3	8	9	3	10	1	0	34
juveniles		2	0	0	0	0	0	2
No. of attacks	46	126	77	88	84	38	31	490
Suspension of criminal prosecution	106	102	121	105	98	93	16	641
Stay of criminal prosecution	24	20	17	24	31	19	6	141
Conditional stay of criminal prosecution	0	1	0	6	0	2	2	11
Indictment/persons	35	36	56	39	58	20	4	248
Final Conviction Cases/persons	8/12	8/11	6/9	11/23	15/22	6/10	4/7	58/94

227. At Prosecution level, no lack of material and human resources in investigating ML was noted. The difficulties are of structural and horizontal nature, related to the effective implementation of financial investigations.

Table 20: Number of persons convicted and acquitted for ML

	CONVICTED PERSONS	ACQUITTALS	LENGTH OF THE PROCEDURE (month average)			
			KP		ÚŠP	
			Pre-trial	Court	Pre-trial	Court
2013	11	0	39	5	N/A	N/A
2014	12	4	49	43	123	13
2015	9	1	53	13	92	34
2016	23	2	25	13	N/A	N/A
2017	22	1	23	19	47	43
2018	10	0	49	35	24	120
30.2019	7	2	40	7.5	44	53
TOTAL	**94**	**10**	**39,7**	**19,4**	**66**	**52,6**

The judiciary

228. The judges met on-site were unanimous in the opinion that the ML legal framework is sufficient to achieve all types of convictions, and that no conviction for the predicate offence is necessary in order to achieve a ML condemnation. Nevertheless, there is still reluctance to pursue ML in the absence of a specific predicate offence and the use of circumstantial evidence to prove the mental element of the offender. It is therefore not surprising that the number of third party and stand-alone ML convictions, although existing, is limited.

229. The judiciary continues to have a strict interpretation attributed to the ML offence and no guidance, recommendations, or example judgements (precedents) were provided in this regard. It was reported that the Supreme Court asks for the repetition of the certain evidence gathered after the charges were pressed and some evidence obtained before the pressing of the charges must be repeated (*e.g.* witness hearing). On a positive note, the practice is in train of being unified with the recent opinion of the Criminal Law College of the Supreme Court allowing the possibility for measures instituted before prosecution to be used as evidence in criminal proceedings. The judges appeared opened to accept various ML scenarios if convinced by substantive training and case examples (including from other jurisdictions).

230. The judges maintained that one obstacle in achieving more numerous and sophisticated ML convictions is the existent disagreement between the law enforcement practitioners, especially about the material element of ML. It remains unclear what type of action should be taken by the alleged criminal for the act to be qualified as ML. An example was given, in which a real estate property obtained illegally was sold and the money deposited in a bank account. This case was interpreted as ML by Prosecution while the Police and the judiciary saw it as a pure fraud case.

231. Another challenge at the judiciary level is the requirement to have a clear distinction between the *"dirty money"* from the *"legal money"*. Therefore, in case of mingled assets/property, a conviction shall be difficult to obtain.

3.3.2. Consistency of ML investigations and prosecutions with threats and risk profile, and national AML policies

Consistency with threats and risk profile

232. The Slovak authorities do not keep statistics on the on-going ML investigations segregated by predicate offences but since the Financial Police Unit NAKA is the LEA being primarily involved

in investigating ML, the convictions follow the profile of economic crimes predicates such as theft, fraud (especially VAT fraud) and embezzlement. This portion of the investigations is somehow in line with the results of the NRA, but not fully consistent with the real ML threats Slovakia faces.

Table 21: ML cases per category of predicate offences[38]

Predicative criminal activities in ML cases[39]								Autonomous
2013	2014	2015	2016	2017	2018	06.2019	Total	
	3		7	1			11	Theft
	2		1				3	Counterfeiting and Alteration of Vehicle Identification Data
	1	1	1	1			4	Fraud
	1	1			1		3	Embezzlement
								Violations of Obligations of Trust
			1				1	Abuse of Authority by a Public Official
						1	1	Counterfeiting and Alteration of Control Technical Measures for the Identification of Goods
			1	1		1	3	Establishment, Plotting and Supporting a Criminal Group
Self-Laundering								
2013	**2014**	**2015**	**2016**	**2017**	**2018**	**06.2019**	**Total**	
2			1	5	1		9	**Theft**
				3			3	**Counterfeiting and Alteration of Vehicle Identification Data**
		1				1	2	**Fraud**
	1	1					2	**Embezzlement**
		1	1				2	**Violations of Obligations of Trust**
			1				1	**Abuse of Authority by a Public Official**
				1			1	**Illegal Production of Narcotic and Psychotropic Substances, Poisons or Precursors, their Possession and Trafficking**
				1			1	**Trafficking**
				1		1	2	**Counterfeiting and Alteration of a Public Document, Official Seal, Official Lock, Official Symbol and Official Mark**
						1	1	**Counterfeiting and Alteration of Control Technical Measures for the Identification of Goods**
				1		2	3	**Establishment, Plotting and Supporting a Criminal Group**

[38] Some cases are counted under more than one line as in the content of the case persons have been convicted for different types of ML

[39] Final convictions

3rd party ML								
2013	**2014**	**2015**	**2016**	**2017**	**2018**	**06.2019**	**Total**	
7	6	1	4	3	2		23	**Theft**
4	4		2	1			11	**Counterfeiting and Alteration of Vehicle Identification Data**
	2	1	1	4	2	1	11	**Fraud**
		1					1	**Violations of Obligations of Trust**
						1	1	**Counterfeiting and Alteration of a Public Document, Official Seal, Official Lock, Official Symbol and Official Mark**
					1		1	**Counterfeiting, Alteration and illegal Production of Duty Stamps, Postage Stamps, Stickers and Stamps**
			1	1		1	3	**Establishment, Plotting and Supporting a Criminal Group**

233. The outcome of investigations and prosecutions of ML in other major proceeds generating offences does not appear to reflect the country risks to the fullest extent. There are some cases where convictions have been achieved for laundering the proceeds of organised criminal groups. Nevertheless, the number of convictions for ML related to organised crime (especially with international ramifications) human and drug trafficking remains modest while the ML cases resulting from theft dominate the statistics. No sophisticated forms of legalization have been identified, *e.g.* using placement of proceeds abroad or by engaging professional individuals and hence, no such convictions have been reported.

CASE BOX 7: "The bank case"

A commercial bank employee performed unauthorized bank transfers from the accounts of a client (victim) in total amount EUR 900 000. In the first stage, the money was transferred in third person's account – opened by the instigator, followed by transfers other accounts owned by other two persons in various banks, one of which was the third perpetrator. Afterwards, via the account holders of these accounts, they made withdrawals of financial means in cash, of which the account holders kept a commission and the rest they handed to the main perpetrators. These perpetrators have used the financial means to purchase various goods and services.

The financial investigation revealed all evidence confirming laundering transaction scheme, as well as property status of all persons involved. During a house search within the investigation, financial means of EUR 449 100 in cash have been seized, which were subsequently returned to the victim bank. The three perpetrators have been convicted for ML with mandatory sentences of deprivation of liberty for 8,5 years (in 2015) and 6,2 years (in 2016). They were also sentenced with the punishment of forfeiture of assets.

234. The VAT fraud is one of the biggest ML threats when the organizers of these crimes directly or indirectly use fictitious directors *("straw-man")* and chains of fictitious companies. Moreover, these phenomena have a direct link with criminal groups in the most serious forms of intra-Community VAT fraud involving neighbouring countries.

235. The establishment of the Financial Police Unit NAKA is closely related to the need to increase the efficiency of activities in the field of combating economic crime, especially tax crime.

As tax frauds drain significant resources from the economy, to which they are invading, thus contributing to the consequences like ML, corruption and organised crime. The Act on Restrictions on Cash Payments (2013) seeks to prevent the issuance of fictitious documents without a real flow of funds. At the same time, by adopting this act, tax authorities have a better overview of entrepreneurial activities and can better concentrate their attention on suspicious transactions.

236. No ML conviction was achieved against a legal entity involved in VAT fraud schemes. The table below gives an overview of the number of VAT registrations withdrawn for being identified as fictitious legal entities involved in VAT fraud schemes.

Table 22: cancelled VAT registrations

YEAR	Number of cancelled VAT registrations according Section 81 (4) b) of Act no. 222/2004 Coll. on VAT
2015	2 355
2016	3 732
2017	3 592
2018	4 167
1.1.2019 – 30.6.2019	1 412
TOTAL	**15 258**

237. One example of an on-going serious VAT carousel fraud case, involving more than 100 legal entities and 60 suspects from different countries who (between 2015 and 2017) withdrew in cash EUR 162 000 000 from seven Slovak banks, raises serious concerns on the ability of the authorities to swiftly react to emerging threats. Moreover, there are no ML indictments in this case which only confirms that systemic vulnerabilities in the AML policy are still to be addressed.

CASE BOX 8: ML and tax evasion case

Predicate offence: Tax evasion (VAT) crime committed by two perpetrators, one of them being charged with ML.

At least during 2017 and 2018 both A.B. and J.B. organized import of large quantities of car tires from Poland selling them to end customers in Slovakia through two e-shops they run. This business was formally covered by two limited liability companies with A.B. being factual BO in both, formally managed by straw-men – homeless persons of Polish and Hungarian origin. The two companies never fulfilled VAT duties resulting from the business here in Slovakia (selling to end customers), while the import of tires from the EU is not subject to VAT. Although they formally declared VAT on the invoice form for the end customers, this was never declared to tax authorities and deducted from the gross income of the companies. This scheme enabled the two e-shops to be the cheapest suppliers of the tires all around and their business could extent to large scale due to the tax evasion. Evaded tax established so far is of EUR 601 782.

Factual basis and ML element: ML- A.B., from 20.04.2018 until 16.05.2018 transferred through 16 transactions the total sum of EUR 206 105 from the bank account belonging to one of the companies involved in the tax evasion scheme to his private account and further disseminated the sum to different bank accounts registered on his family members. There is a strong suspicion of investing the proceeds of the "business" by A.B. to real-estate purchase – it is foreseeable that the scale of ML will extend as the investigation goes on.

Identification of the case (relevance to IO 7): The tax case was triggered by the criminal complaint of a private person. ML case was uncovered during the course of investigation. During

the FI was established evidence in relation to: Bank accounts – in cooperation with FACO operatives, real estate register, commercial register.

Property seizure and freezing (relevance to IO 8): 4 bank accounts secured through § 95 CCP – the sums so far secured: EUR 3 428; EUR 131; EUR 79 577; EUR 129 374. The cash secured during home searches: EUR 87 473, USD 570, and 3 660.

One newly built apartment secured by the decision of the prosecutor under § 461/2 CCP – the value of EUR 15 676, (the cost of construction, not the market value). The apartment was formally registered on A.B's father but the construction was financed by A.B. from the proceeds of crime – more real estates are expected to be secured, as their construction and the ownership of A.B.'s relatives are expected to be registered.

Status of the case: ongoing (Regional criminal police and regional prosecution office)

238. Corruption in broader sense constitutes a medium-high threat. Between 2013 and 2018, 671 of corruption convictions have been reported. However, tangible results in prosecuting and convicting corruption related ML cases have not been achieved, and very few on-going investigations have been reported. The authorities argue that *"the bribes were paid in cash or even by a bank transfer, but without any effort to hide it through a fictitious act",* which only demonstrate the high level of threshold self-imposed in ML cases *("hiding through a fictitious act")* and the limitations in understanding all forms of ML offence. Another typology concerns bribes which are provided in the form of invoiced payments for various fictitious services, goods and activities, where there is a clear track in the accounting documents and bank records, but for which investigators need a longer period of time for investigations.

Consistency with national AML policies

239. At strategic level, steps have been taken by the authorities to promote the ML as one of the high priorities for the law enforcement community.

240. In May 2019, following the adoption on the NRA, the Government adopted the AP to combat legalization of proceeds of criminal activity, terrorist financing and financing of proliferation of weapons of mass destruction for 2019 – 2022, which includes *"orders"* and *"recommendations"* for the key stakeholders in the AML/CFT area, including the MoI, the MoF, the MoJ and the GPO and the NBS. Some of the *"orders"* are of a very general nature such as to reduce the level of social acceptability in the area of generating illegal proceeds and their placement in the legal economy, while others are more specific such as to introduce a full proactive parallel financial investigations and intensify the training provided to LEA officers in this respect.

241. The AP recommends the LEA to strengthen the use of intelligence to identify the proceeds of criminal activity from the earliest stages, and to prepare operational procedures for investigating legalization of proceeds of criminal activity. The GPO should assist in identifying and developing relevant typologies of the most frequently misused sophisticated schemes of legal entities with an emphasis on the cross-border aspect.

242. In the implementation of the AP, on 3 June 2019, the General Prosecutor adopted his own *"Measure of the Prosecutor General implementing NRA"*. Measure elaborates in detail every task of the AP pertaining to the prosecutor's service. This document contains the tasks that the GPO carries out autonomously, but also determines the arrangements and the way of ensuring key tasks in situation where GPO is only a position of cooperating entity.

243. The AT commends the authorities for the adoption of the AP and the other policy

documents which in its content demonstrates the awareness on the shortcomings and challenges encountered in relation to the effective investigation and prosecution of ML cases. Nevertheless, at the time of the on-site visit, remained at policy level, without visible impact on results.

244. In addition to the AP, and as a result of the NRA, in 2019, the *"Strategic Principles for Combating Money Laundering, Terrorist Financing and the Proliferation of Weapons of Mass Destruction for 2019-2024"* were adopted, which is a binding management document for all state administration bodies.

245. In March 2015, prior to the adoption of the NRA, the GPO prepared an *"Information paper"* for the General Prosecutor on the *"Assessment of effectiveness in the activity of the GPO in the field of criminal prosecution of ML and seizure of proceeds of crime"*. The document highlighted most of the deficiencies identified by the AT such as: limited trained staff and technical tools to document a ML cases; lack of systematic use of financial investigations; lack of sufficient training of judges and insufficient court practice; shortcomings in the execution of seizure of property in the initial stages of criminal proceedings etc… The practical results of the Information Paper is the adoption of the Methodical Guidance on financial investigations, issued in 2017 as well as action plans conceptually related to ML: the action plan to combat tax fraud, to combat terrorism, to combat illegal migration.

246. SR has introduced some policy measures to address corruption, such as the Anti-Corruption Policy 2019-2023, approved by the Slovak Government in 2018, where the issue of financial investigations is mentioned but no reference is made to ML.

247. Although the AT acknowledges the documents and coordination meetings held in relation to the practical implementation of a more effective approach in ML investigations, a national ML-specific enforceable operational policy is needed to ensure a more uniform and effective approach across all LEAs involved.

3.3.3. Types of ML cases pursued

248. In the period of assessment, the Slovak Republic achieved 94 ML convictions the majority of which were instrumented in parallel with the predicate offence. There is still a reluctance to pursue ML in the absence of a specific predicate offence and the use of circumstantial evidence to prove the mental element of the offender, although some cases do exist.

Table 23: Types of ML convictions

Year	Cases/Persons	Self-laundering	Autonomous ML	Third party ML
2013	8/11	3	0	8
2014	8/12	3	2	7
2015	6/9	2	4	3
2016	11/23	3	9	11
2017	15/22	8	6	8
2018	6/10	2	2	6
06.2019	4/7	3	1	3
TOTAL	**58/94**	**24**	**24**	**46**
			94 persons	

249. While legal entities are said to be frequently used as vehicles for ML, the assessors note that no legal persons have been convicted for ML. Since the introduction in the Slovak legislation on the criminal liability of legal persons, numerous convictions have been achieved for other crimes, which cannot constitute a positive element in the importance granted to ML vs. other

criminal acts.

Stand - alone ML (autonomous), 3hd party ML

250. The cases and the interviews demonstrated that it is possible to prosecute autonomous ML, without a conviction of the predicate crime. In case of foreign proceeds, the judiciary confirms that there is no need for a prosecution or conviction of foreign person or for the foreign predicate offence to indict persons in Slovakia for autonomous ML, if the evidence on predicate offence is solid.

251. However, the number of convictions remains modest when compared to the number of ML investigations, the number of convictions for the predicate offences, and the overall country risks. In practice, most of the stand-alone prosecutions relate to stolen cars, and where the perpetrator either registers higher number of stolen vehicles or he offers implausible sources for their acquisition. The Slovak LEA need to strengthen the investigations on more sophisticated autonomous ML, commensurate with the country's risk profile, including complex VAT frauds, corruption and international organised crime.

252. To accelerate the finalisation of ML pending cases, a compilation of Court practice, for all types of ML convictions achieved so far, is needed as guidance. It is also important that prosecutors are made aware of these case studies.

CASE BOX 9: Example of third-party ML

Predicate offence: Theft of footwear in Austria

ML element: It was a case of autonomous ML in the territory of the Slovak Republic, where at that time the perpetrator was not convicted for a predicate criminal offence. The offender obtained footwear as a freelancer whereby he was aware that it originates from the theft of 1 837 pairs of shoes worth of EUR180 000, which took place in Austria. He has sold 842 pairs of shoes for EUR12 500 Eur to another person in SK. 565 pairs of shoes worth EUR9 565 have been seized in SK during the transfer to Czech Republic, where he wanted to sell them. He has kept hidden 287 pairs of shoes in another place in SK until their seizure.

The court has referred to direct evidence and a continual chain of indirect evidence. On the subjective side, the court has affirmed that the perpetrator may be unaware of the specific criminal activity from which the item originates. It is enough though he is aware of the facts from which one may reach such conclusion on the criminal origin of the item, even if by collusion. It is a conduct consisting of a concealment of origin of goods in the criminal offence, seeking to appear as a lawful acquisition.

Identification of the case (relevance to IO 7): The case was instigated based on the results of operative activity of the investigator of the Regional Directorate of the Police Force. During the criminal intelligence investigation action with the aim to establish cross-border nature of crime were performed, persons in question were identified. Within the financial investigation, the investigator has obtained bank account statements of the accused, as well as records from the real estates' register and of motor vehicles as well as movement of funds were established.

Based on the request, the Austrian judicial authorities have provided effective legal assistance. They have stated that the investigation of theft was not terminated yet. A lost mobile phone was seized at the place of the theft of the footwear where the DNA of offender was found. It was established that in the morning following the theft of the footwear, the said person was already offering by phone the sale of footwear with fake documents and invoices. As evidence were used

testimonies of the transferring drivers, of a buyer of the footwear and of controlling customs officers, further recognitions, documents of the footwear, records on the movement of vehicles of customs' gates, outcomes of house searches and searches of other premises, transcriptions of telecommunication activity made, SMS messages, e-mails, expert's opinion from the Department of Electro-technology concerning the laptop of the convicted and the fake invoices and image files containing photographs therein obtained, and by determining the localization data on the residence of the aggrieved party as well as outcomes of legal assistance.

Property seizure and freezing (relevance to IO 8): The entire seized footwear in Slovakia during house searches and searches of other premises (three different places/in 3 cities - 842 pairs, - 565 pairs and 287 pairs of shoes) was during the criminal prosecution returned to the injured party to Austria pursuant to Section 97 (1) of the CCP.

Status of the case: In 2017, by the judgement of the District Court Zvolen, the indicted RM was found guilty of committing a continuing ML, partially in the stage of an attempt. For the above-stated offence, RM was imposed a punishment of deprivation of liberty of 4 years and 6 months, and the forfeiture of items pursuant (incl. instrumentalities used for committing a crime e.g. notebook, etc.).

Geographic factors of ML and foreign element

253. According to the NRA, 1 113 Slovak nationals were involved in ML cases, representing a 95,54% share of the total number of ML cases (the total of 1 165 cases considered for NRA purposes included the *"sharing"* crime, see IO7.5); while foreigners were involved in 53 cases (8,50%).

254. From the NRA it results 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%). Other target countries were 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 were Germany, Austria, the Czech Republic and Italy.

255. The authorities provided examples of ML convictions with foreign predicates (see CASE BOX 5 above). Nevertheless, the data and statistics demonstrate that there is misperception when it comes to the external element in relation to ML cases. In some instances, the *"external element"* is considered to be the nationality of the perpetrator, while in others, the origin of the proceeds. To add up to the confusion, in the Table 24 below, the place of the commitment of the ML is considered, while the relationship with the SR in *"ML cases committed abroad"* is unclear.

Table 24: Regional aspects of the origin and placement of proceeds of crime (convictions/cases)

2013-2018		
Place of committing ML	**ML – committed on the territory of the SR SK**	178
	ML – committed abroad	7
	ML – committed partially in the SR, partially abroad	CZ – 2, SK– 15, AT – 3, IT – 2, BG – 1 HU – 2, CH – 1, MT – 1, USA – 1, other – 35 (undetected)
	The country cannot be precisely determined	13
Number of participating Slovak natural/legal persons		214/0
Number of participating foreigners		28 CZ – 4, UA – 3, HU – 13, RO – 3, IT – 3, BG – 1, PT – 1, FR – 1, Other – 5 (undetected)

256. It is difficult to measure the impact of the external element in ML cases in Slovakia due to deficient data and statistics kept. For example, in the Table 25 below, all the ML cases are boiled together per year making it difficult to draw a meaningful conclusion on the foreign proceeds laundered in Slovakia as opposed to proceeds obtained domestically and laundered abroad.

Table 25: ML cases disaggregated by origin of proceeds.

2013-2019 (up to 30/06/2019)		
YEAR	**Country of Origin** (the country where proceeds of crime where generated)	**Country of Destination (**the country where the proceeds of crime were directed or placed or legalised)
2013	2x CZ; 4x SK; 1x AT; 1x IT	7x SK 1x Planned to be placed in UA
Volume of laundered proceeds	EUR69 515 + in 3 cases the value was not exactly determined	
2014	2x AT; 5x SK; 1x CZ	8x SK
Volume of laundered proceeds	EUR274 261 + in 1 case the value was not exactly determined (1x car)	
2015	4x SK; 1x SUI	4x SK; 1x UA
Volume of laundered proceeds	EUR968 471	
2016	7x SK; 1x AT; 1x IT; 1x HU; 1x ESP	11x SK
Volume of laundered proceeds	EUR1,172,170 + in 1 case the value was not exactly determined (apprx. 100 cars)	
2017	7x SK; 2x UA; 1x CZ; 2x AT; 3x IT; 1x ESP; 1x USA	15x SK; 1x UA
Volume of laundered proceeds	EUR1 693 827 + in 4 cases the value was not exactly determined (4x mobile, notebook, chain of banking operations)	
2018	4x SK;1x CZ;1x AT	5x SK; 1x CZ
Volume of laundered proceeds	EUR960 306 + in 2 cases the value was not exactly determined (3x cars, valuable stamps)	
2019	Cayman Islands; China; Mongolia; 2x SK; USA; CZ	Poland; China; UK; 3x SK; USA
Volume of	EUR3 211 653 + in 1 case the value was not exactly determined (chain of banking	

laundered proceeds	operations)	
Total	**6x CZ;32x SK;7x AT; 5x IT;1x SUI; 1x HU;2x ESP;2x UA;2x USA; 1x Cayman Islands; 1x China; 1x Mongolia**	**53x SK; 1x Planned to be placed in UA; 2x UA;1x CZ;1x Poland; 1x China; 1x UK; 1x USA**
Volume of laundered proceeds	EUR8 350 208 + in 12 cases the value was not determined (105x cars, 2x parts of cars, 4x mobile, 1x notebook, stamps)	

3.3.4. Effectiveness, proportionality and dissuasiveness of sanctions

257. The sanctions applied for ML offences mainly consist of custodial sentences. There are no ML convictions against legal entities, while for other crimes, 15 convictions have been achieved since the criminal responsibility of legal persons has been introduced in 2016.

258. The imprisonment sanctions imposed for ML appear to be effective, although it is noted that most convictions result in sentences at the lower end of the scale (confirming the tendency to pursuit simple ML offences as described under 7.2 and 7.3 above). In 2015-2017, the ratio between the executed prison sentences and suspended sentences was of 50%-50%, while in 2013-2014 and 2018 significantly more sentences were suspended. The imprisonment time is in average of 30 months, while suspended sentences (applied in 47 cases including 16 Autonomous/Third party ML) average 33 months.

259. The sentences pronounced so far are proportionate as the courts imposed high penalties for serious offences such as organised criminality and ML, where the accused persons were sentenced to 16- and 21-year imprisonment.

260. On a less positive note, the fines applied so far do not appear to be dissuasive enough (average EUR675), with one notable exception where a penalty of EUR20 000 was imposed (all fines were imposed in self-laundering cases). The fines are generally lower than the laundered amounts. Other penalties were also imposed, such as radiation of legal persons or expulsion.

261. The level of dissuasiveness of the sanctions is moderate, mirroring the profile of the convictions achieved so far, which are rather simple ML cases. For other serious crimes, higher average sentences have been pronounced: 185 months for organizing criminal groups, 71 months for drug and psychotropic trafficking, 76 months for trafficking and smuggling, 69 months for currency counterfeiting. The average sentence for ML is limited to 30 months. The AT is confident that enhancing the profile of the ML into more serious and complex cases will lead to the application of more dissuasive penalties.

262. In overall, the AT concludes that penalties are effective and proportionate, given the types of ML pursued. Turning to dissuasiveness, the prison sentences should follow the seriousness, the gravity and consequences of the crime committed, and the suspended penalties should be carefully considered and justified. Where milder prison sanctions are imposed the dissuasiveness should be maintained through other means (*e.g.* dissuasive fines). Property sentences are sometimes applied cumulatively with the prison sentences.

Table 26: Penalties for ML alone or/and cumulative with other crimes

Year	Non-custodial sentences		Custodial sentences	
	Highest	Lowest	Highest (months)	Lowest Prison Sanction (months)
2013	FORFEITURE (Items)	-	88	WAIVING the Multiple Punishment and Additional Penalty § 44 CC
2014	FORFEITURE (Items – stolen car)	Monetary Sanction 200	40	24 (24 suspended)
2015	FORFEITURE of all property	Monetary Sanction 20 000	102	24 (26 suspended)
2016	FORFEITURE of all property	Monetary Sanction 300	156	WAIVER OF PUNISHMENT
2017	FORFEITURE of all property	Punishment by Disqualification or Deportation	255	WAIVER OF PUNISHMENT
2018	FORFEITURE (Items)	Punishment by Disqualification	60	24 (24 suspended)
06.2019	FORFEITURE of all property	FORFEITURE (Items)	252	96

3.3.5. Use of alternative measures

263. In cases of *"in absentia"*, failure of cooperation of the foreign judiciary body, missing person, the death of the suspect, etc., there are a range of measures which can be deployed. The same apply when ML prosecutions are unavailable for other reasons (*e.g.* for lack of sufficient evidence). In practice, when the ML offence cannot be included in the indictment, authorities prosecute for other offences (preferably predicate offences and tax offences).

264. The country applies other criminal justice measures when it is not possible to secure a ML conviction. In certain cases, the crime of *"sharing"* is retained as reflected in Art. 231 of the CC as a form of ML which criminalizes simple possession and use of criminal assets by third person (other person than offender of predicative criminality) having knowledge about the criminal origin of such a property and without any other intention to hide and change its origin. As discussed in the TCA, this a more traditional, receiving-type offence which partially overlap with the ML offence. However, its generally limited scope resulted in a practice where *"sharing"* is represented by low-profile criminality, without producing serious forms of ML and volumes of criminal assets.

Table 27: Convictions for the *"Sharing"* crime

SHARING							
	2013	**2014**	**2015**	**2016**	**2017**	**2018**	**Total**
Commencement of criminal prosecution	64	58	128	29	99	101	**479**
Terminated Criminal Prosecution of Unknown perpetrators	33	33	29	35	32	31	**193**
Persons accused	216	161	117	78	83	74	**729**
Finalized criminal Prosecution of Accused Persons	231	206	129	132	97	82	**877**
Women	33	37	13	12	19	20	**134**
Juveniles	26	20	20	12	14	9	**101**

No. of attacks	247	219	130	134	111	103	**944**
Suspension of criminal prosecution	26	33	20	20	23	15	**137**
Stay of criminal prosecution	29	55	25	25	29	28	**191**
Conditional stay of criminal prosecution	14	17	9	3	2	5	**50**
Conciliation	2	1			1		**4**
Indictment – persons	138	90	81	78	74	68	**529**
Agreement on guilt and punishment	32	31	21	27	7	1	**119**
Final Conviction	123	124	77	86	54	23	**487**

265. The majority of the cases above generated assets of "petty crime" nature, or assets were either consumed by the perpetrator or, at maximum, just used or possessed by a third person.

266. Apart from the situations above, other criminal justice measures should be favoured by the Slovak authorities in cases where a ML investigation has been pursued but where it is not possible, for justifiable reasons, to secure a ML conviction. This may include use of extended confiscation, confiscation without prior conviction, utilisation of administrative sanctions and referrals to supervisory bodies for potential revocation of operating licences.

Overall conclusions on IO.7

267. Although the number of investigations and prosecutions for ML are on the rise, the results in terms of effective ML investigations and prosecutions remain low. There is no specialised LEA in handling ML cases which are to be dealt with by the authority having competence over the predicate offence. In practice, financial investigations are not routinely done. Investigations of ML cases related to economic crimes are consistent with the country risk profile as depicted in the NRA, but not with the country's threats due to shortcoming in the NRA. Investigating and prosecuting ML is in line with national policies and plans. Slovakia to some extent prosecutes and convicts different types of ML cases. Courts imposed effective and proportionate sanctions. The authorities have a range of other criminal measures which can be deployed where it is impossible to secure a ML conviction.

268. **The Slovak Republic is rated as having a Moderate level of effectiveness for IO.7.**

3.4. Immediate Outcome 8 (Confiscation)

3.4.1. Confiscation of proceeds, instrumentalities and property of equivalent value as a policy objective

269. The complex system of property-related measures, by which ill-gotten assets are targeted, remained largely unchanged both in the CC and CCP and offers a range of robust instruments for the authorities. Some of these measures (such as the forfeiture of assets) however, fall beyond the scope of FATF standards, which makes it difficult to assess separately the effectiveness by which proceeds and instrumentalities of crime are seized and confiscated.

270. Slovak LEA and Prosecution have demonstrated that seizure of criminal proceeds and instrumentalities had been in the centre of their attention throughout the assessed period. In general terms, this issue is conceptually included into the systematics of financial investigation, in which area several measures were issued, and various specified analyses were performed. As opposed to the performance of the provisional measures' regime, however, the assessors could not obtain meaningful information regarding the confiscation of criminal proceeds and

instrumentalities, let alone the volume of confiscated assets that have successfully been recovered.

271. As discussed already under IO.7, financial investigations should theoretically be carried out in all criminal cases related to proceeds generating offences and particularly to those which carry property forfeiture as an obligatory punishment. Investigating authorities enjoy procedural autonomy in adopting decision on the scope of a financial investigation as well as in detecting, identifying and securing criminal assets and instrumentalities, assisted and instructed by the competent prosecutor using their rights and power of supervision in line with the general prosecutorial guidance issued in this field.

272. In the two Methodologies of 2017 that the investigative and prosecutorial practitioners used in the time period relevant for this assessment, the basic objective was stated as *"identification, monitoring and seizure of the proceeds from criminal activity and of other property, which could be subject to property-related sanction, whereas it focuses equivalently on the property belonging to the suspect, which could be transferred to the third parties"*[40]. As it was explained by representatives of the GPO, taking into account the organisational and material conditions, as well as aspects of proportionality and effectively of criminal prosecution, financial investigations are carried out at two basic levels, where the primary action consists of detecting and proving evidence of the proceeds coming from criminal activity as well as elaborating the proprietary profile of suspected perpetrators, while more complex activities should then be a part of extended financial investigation. In this context, the Methodology specified the basic part of prosecutorial activities as the earliest possible and permanent investigation of conditions for seizure of the property of the item in all their forms with the aim to prevent its evasion, for the purpose of its future confiscation, or for the purpose of securing damages of the injured party, also including determining of facts related to the question whether there is a concern that enforcement of the confiscation measures or of securing damages of the injured party would be thwarted or hindered. Increased attention must be paid to identification and taking evidence of the facts for the purpose of fulfilling conditions to apply elements of confiscation without previous conviction (Art. 83 CC).

273. As compared to the time of the previous evaluation, the use of parallel financial investigations has since yielded some notable results in seizing assets in the investigative stage of criminal proceedings. This is particularly true for the number of cases where provisional measures (most notably, the seizure of money on bank accounts) were applied as well as to the volume of assets secured by such measures.

274. The regular and effective application of financial investigations is however hampered by several factors, starting with the logistical and procedural constraints at certain LEAs (particularly within the Criminal Police). Financial investigations are generally to be carried out by the investigator being in charge for the criminal investigation itself (as it would be the case in Criminal Police investigations) except within the activity of NAKA units, where it is performed by the ARO NAKA (by virtue of Instruction 51/2017 of the NAKA Director). For NAKA units, the ARO would carry out financial verifications and elaboration of property profiles for the purpose of thorough application of Art. 119 (1) f CCP or for other purposes *e.g.* securing damages of the injured parties. However, there is no dedicated body to assist all investigators in this field as ARO NAKA's assistance is not available for all LEAs unless in cases with an international aspect (where property

[40] In the 2019 GPO Methodology, this is complemented by other objectives such as determining the extent of national and transnational criminal networks and the extent of crime, disrupting OC structures particularly in the context of ML/FT and creating of conditions for a commencement of the criminal proceedings.

needs to be identified and secured abroad) or on an ad hoc basis, depending on the decision of the director of the NAKA. In order to overcome this deficiency, two financial investigation analysts were deployed to each regional Police Directorate as from 01 October 2019.

275. One of the main challenges identified by LEAs in this area is how to elaborate, at the earliest stage of the proceedings, the property profile. As it was expressed onsite, elaboration of such profiles is time demanding which has often allowed perpetrators to successfully dispose of their property with the objective to avoid the risk of confiscation by simulated transfers to third parties. Difficulties in this field are, at least partly, attributable to the general lack of proceeds-oriented operative analysis in the pre-investigative (operative) phase of the proceedings.

276. Transfer of criminal assets by the perpetrator to third parties was recurrently mentioned by LEAs as a general obstacle to effectively seize and confiscate such property considering the practical inapplicability of Art. 425 CCP in such cases. As it was explained, at least some LEAs considered this provision to only allow for seizing the property of, or property right belonging to the defendant at the time of the seizure, with no legal possibility to seize property registered on other persons, even if the accused demonstrably used it. As a consequence, these LEAs do not have the legal possibility to contest retroactively the transfer of the property during the financial investigation, even if it could have been demonstrated that such transfer had been made on purpose, to avoid the confiscation of such property. Another issue mentioned in relation to Art. 425 CCP was the high evidentiary standards required for this preventive measure, the application of which requires evidence of reasonable concern that execution of the punishment would be obstructed or hindered.

277. Subsequent to the on-site visit, the Slovakian authorities explained that Art. 461(2) CCP read together with Art. 83 CC does provide for seizing proceeds of crime from third parties, already in the stage of pre-trial investigation, with a view to subsequent confiscation of such assets or items. The authorities claim they regularly use this method to secure assets the perpetrators have transferred to third parties and thus the deficiencies described above do not exist. Indeed, a case example was provided which convincingly demonstrated the applicability of Art. 461 (2) CCP in such circumstances. In this case, a newly built apartment was seized pursuant to this provision, which apartment was formally registered as property of the defendant's otherwise uninvolved father, but the construction of which had actually been financed from the proceeds of the crime the defendant had committed.

278. Having said that, the information provided both in the MEQ and during onsite interviews clearly implies that at least some of the competent LEAs have not considered the existing legal framework being applicable to seize criminal proceeds from third parties which necessarily means that these authorities have not implemented the confiscation and provisional measures regime in this respect. This is an issue of effectiveness even if not caused by technical deficiencies but by the inadequate understanding of the legal framework. Furthermore, the other deficiency mentioned in relation to in Art. 425 CCP that is, the overly high evidentiary standard is not at all mitigated by Art. 461 CCP which reiterates the same wording as used in Art. 425.

279. When asked whether they have adequate resources to perform their functions, NAKA units and prosecutorial authorities expressed that such resources were sufficient, however other answers in the MEQ as well as information the assessors obtained onsite appear to prove certain issues in LEAs such as the Office of the Criminal Police, where financial investigation and property profiling has been done by the criminal investigator of the underlying criminal offence, with an apparent impact on their effectiveness in identifying and securing of property.

3.4.2. Confiscation of proceeds from foreign and domestic predicates, and proceeds located abroad

280. The overall figures for final property decisions applied in criminal cases (including all forms of criminal forfeiture and confiscation) are generally low, which is particularly true for ML cases. Forfeiture of property has only been applied in 13 ML cases throughout the assessed period of 6 ½ years. It needs to note, however, that this form of punishment was not applied too frequently for other crimes either (98).

281. The forfeiture of property as a punishment measure, while undoubtedly a powerful tool for confiscating potential criminal proceeds inasmuch as such proceeds are included in, and thus constitute an indefinite part of the entire property of the defendant (as there is no need to demonstrate exactly which part or what proportion of that property has been derived from crime) it appears to go beyond the FATF standards and makes it difficult to separately determine what proportion of actual criminal proceeds and instrumentalities have been confiscated.

282. Forfeiture of an *"item"* was applied quite often in criminal cases not involving ML charges (821 to 975 cases per year) but surprisingly rarely in ML cases, which means 4 occasions throughout the entire time period. This measure would also serve for confiscating proceeds of crime (property items which the offender has obtained by a crime or as a reward for it, as well as the corresponding value thereof) but analysis of the statistics implies that it is essentially applied to forfeit physical objects used as instrumentalities for a crime, which is less characteristic for ML cases. The confiscation of a *"thing"*, which is basically a form of in rem confiscation of criminal proceeds and instrumentalities, shows a moderately frequent use in cases not involving ML charges but, again, an extremely rare occurrence in ML cases with only 2 examples throughout the period of assessment.

Table 28: Confiscation of property decisions

Confiscation								
		Case	Number					
			2013	2014	2015	2016	2017	2018	2019 (30.06)
Forfeiture of property	§ 58 CC	ML	0	0	1	4	5	2	1
		other	9	4	24	15	23	23	8
Forfeiture of thing	§ 60 CC	ML	1	0	0	1	0	1	1
		other	975	968	870	821	855	863	298
The confiscation of the thing	§ 83 CC	ML	0	1	1	0	0	0	0
		other	84	54	94	51	63	71	20

283. Beyond the general figures mentioned above, the statistics relating to the confiscation regime are not sufficiently comprehensive to follow the efficiency of the confiscation measures and the lack of basic information practically prevented the AT from carrying out a more thorough analysis of its effectiveness. As opposed to statistics on the provisional measures' regime, there is a

general lack of information on the value or volume of property or property items subject to confiscation. In addition, the statistics on the forfeiture or confiscation of a thing do not specify whether if any of the assets confiscated in such regimes constituted proceeds of crime or equivalent value (admitting, on the other hand, that proceeds of crime are often covered by the more inclusive measure of forfeiture of property under Art. 58 CC). As a result, the assessors were provided with no information to determine (or even to estimate) the ratio between the seized and confiscated assets, that is, what proportion of criminal proceeds secured in the investigative stage has finally been confiscated, as well as the value of the confiscated property that has been effectively recovered.

284. Subsequent to the onsite visit, some pieces of additional information were provided but these only allow for a very limited insight into the performance of the confiscation regime. In the table below, one can see the volume of seized assets on the one side (as approximately as the value of non-pecuniary assets can be estimated) while property that has been effectively recovered on the other. Unfortunately, there are still no figures available on the volume of confiscated/forfeited assets, only the number of the respective measures (sanctions) taken by the court.

TABLE 29: Seizure vs property sanctions vs real deprivation of criminal assets (real recovered)

Year	SEIZURE		Property sanctions (value not identified)				Real recovery
	Money secured on bank accounts	Other secured property	§58 CC	§60 CC	§83 CC	Total	
2013	EUR 10 691 407	EUR 1 177 175 CZK 23 400	9	976	84	**1069**	EUR 116 127
2014	EUR 5 911 210	EUR 4 562 495 HUF 34 000	4	968	55	**1027**	EUR 304 872
2015	EUR 6 667 148 CZK 23 800	EUR 2 424 330 USD6 CZK 516 540 GBP 85 HUF 1 336 000	25	870	95	**990**	EUR 267 886
2016	EUR 8 495 462 CZK 292 947	EUR 1 032 541 CZK 3 135 USD1	19	822	51	**888**	EUR 71 835
2017	EUR 20 241 070 CZK 2 000	EUR 3 010 267 275 861 HUF CZK 74 000	28	855	63	**946**	EUR 76 197
2018	EUR 61 281 501 BTCN 161,90957883	EUR 59 932 247 HUF 4 000	25	864	71	**958**	EUR 1 957 672
Total	**EUR 113 287 802 CZK 318 747 BTCN 161,90957883**	**EUR 72 139 057 CZK 617 075 HUF 1 382 000 USD7 GBP85**	**110**	**5355**	**419**	**5884**	EUR **2 794 591**

285. What can be compared from the above, incomplete table is thus the approximate volume of seized assets versus the volume of confiscated property that has been recovered. This table can only serve some very basic illustrative purposes, as it does not differentiate between proceeds and instrumentalities (let alone cases where the entire property of the defendant is forfeited). In addition, some instrumentalities are not included in the figures (items that were subsequently destroyed) and the last column does not include property items that have been recovered, but

were then taken over by the state as part of the execution of the property decision (*e.g.* a forfeited house that was turned into a public kindergarten).

286. Having said that, one can still notice that the ratio between the assets secured and those recovered is enormous. In terms of the total figures for the entire period, not more than approximately 1.5% of the seized assets became subject of asset recovery (considering only the comparable EUR values) which is negligible. The authorities argued that a significant part of the seized property had been returned to the victims of the (predicate) crimes, but the actual proportion of such assets could not be verified. In lack of more information regarding the confiscation regime, the AT was not in the position to determine all aspects of the aforementioned anomaly.

287. Lack of information in this respect could only partially be remedied by case examples intended to illustrate the effective application of the confiscation measures. Most of the case examples were related to the application of forfeiture of property as a punishment which, as mentioned above, might indeed be considered a powerful instrument to confiscate all property owned by the perpetrator of a proceeds-generating crime regardless to whether and what proportion of that property would have actually constituted criminal proceeds. On the positive side of this feature, the authorities need not to bother with bringing evidence for the criminal origin of the assets of the perpetrator. On the other hand, the success of this measure is determined by the effectiveness of the financial investigation, from the property profiling of the perpetrator to the application of provisional property measures. As noted elsewhere, the forfeiture of property has reportedly been regularly evaded by criminals who transfer their properties to third persons by false documents which, at the same time, appears to demonstrate the ineffectiveness of the entire regime as regards third party confiscation.

288. In case the financial investigators fail to identify all property items that belong to the perpetrator, this failure will unavoidably restrict the scope in which property forfeiture can be applied by the court. Furthermore, if no property was identified and secured during the proceedings, then the identification of any property can only take place in bankruptcy procedure which, as it was demonstrated during the onsite visit, has limited opportunities to secure property. It needs to note, also in light of the case examples provided in relation to the application of property forfeiture, that there are neither statistics nor any estimations available so as to determine the volume of assets recovered as a result of property forfeiture in cases where no previous measures have been taken to secure the assets of the defendant, particularly as in many of those case examples the assets the authorities could secure during the investigation were used for (otherwise justifiable) victim compensation purposes.

CASE BOX 10: Victim compensation precedes forfeiture (ATM case)

In a criminal case tried by the Regional Court in Prešov, five perpetrators were sentenced for a particularly serious crime of theft in 2016. The factual basis of the case was that the defendants, as members of an organized group, after long and sophisticated preparation, entered ATM rooms where they stole funds totalling EUR1 936 600 from 14 ATM devices. During the investigation, it was not possible to trace and secure the stolen funds, but according to Art. 50 CC, the claimant bank was entitled to compensation of the damage by the otherwise legitimate property of the accused (family houses, flats, gardens and land of the perpetrators) in the amount of approximately EUR710 000. In addition, the three main members of the organized group were sentenced to imprisonment as well as forfeiture of property punishment under Art. 58 CC.

289. In the case example above, all available property of the defendants was secured for the purposes of compensation of the victims. While this is a commendable approach in itself, the simultaneous application of the forfeiture of property as punishment in cases like this appears rather mechanistic and thus futile (as there will be no property left for forfeiture).

CASE BOX 11: Confiscation from a legal entity

In a criminal case tried by the District Court in Prešov in 2016 (second instance verdict in 2018) related to VAT fraud, the factual basis of the case was that the defendants, as members of an organized group, created a multi-company special-purpose chain in which they pretended to trade food products (sugar and oil) based on false accounting and tax documents, and thereby reduced the VAT totalling EUR 1 557 864. The perpetrators were sentenced to imprisonment and one of them also to the forfeiture of property (Art. 58 CC.) During the investigation, funds were secured in the account of a legal entity (part of the chain of commerce) in the amount of EUR 22.917 which were confiscated in the sentence pursuant to Art. 83(1)(c) CC (the legal person was not prosecuted for the sole reason that the Law on Criminal Liability of Legal Entities came into effect after the commission of the respective criminal offence.) In addition to that, EUR 44 000 and EUR 160 000 were secured in cash from the 2 perpetrators as result of home searches, out of which the sum of EUR 44 0000 was eventually released but the 160 000 became part of the property subject to forfeiture.

290. What is however clear in the statistics is that neither of the aforementioned property decisions has regularly, if at all, been applied in ML cases, which is in a striking contrast with the frequency by which bank account money, cash and securities as well as real estate and other property items are seized in course of financial investigations by LEA. Considering that the only property decision demonstrating a more frequent application (forfeiture of a thing) is likely to cover, as discussed below, mostly physical instrumentalities, one can conclude that the Slovak Republic could not demonstrate the capability of the confiscation regime to successfully forfeit or confiscate proceeds of crime. This can only partly be affected by the fact that significant volumes of assets secured during the investigations are reported to be eventually returned to the victims of the (predicate) crimes (and thus exited the confiscation regime) particularly as the AT were not given comprehensive statistics in this respect. This is in striking difference from the frequency and volume by which property-related provisional measures have been applied in the assessed period (as demonstrated by prosecutorial and law enforcement authorities) and indicates serious issues stemming from either the overly high evidentiary standards applied by the judiciary (as it appears to be the case concerning Art. 425 CCP) or the inaccurately large scope in which provisional measures are taken.

TABLE 30: Provisional measures to secure bank account money for the entire Prosecution Service (euro if not mentioned otherwise)

		2013	2014	2015	2016	2017	2018	06.2019	TOTAL
Securing of damaged party title	ML		2 477 252	3 1458 698					**5** **1 935 950**
	FT								

	Other	6 1 158 983		1 57 874		2 282 654	2 39 047 000	2 18200 000	**13 58746 511**
Seizure of monetary funds	**ML**	4 8 286 340	29 3239 194	21 3198 437	35 6 078 580	19 2 928 751	14 1 182 063	7 351 049	**129 25264 417**
	FT								
	Other	18 1 146 083	15 580 514	22 1613 201 + CZK 23,800	25 2 247 882 + CZK292 947	26 15 595 002 + CZK 2 000	24 1 500 648	14 332 236	**144 23 015 568 + CZK 318 747**
Seizure of booked	**ML**								
	FT								
	Other		1 500 000						**1 500 000**
Seizure of property	**ML**		1 1104 250			2 99 966	2 10 008		**5 1 214 224**
	FT								
	Other	1 100 000	1 10 000	3 338 937	3 169 000	3 1 334 696	9 19 541 781 (of which 1 is undefined value)	2 650 000	**22 22 144 414**
Item seizure	**ML**								
	FT								
	Other						1 161,90957883 BTCN		**1 161,90957 883 BTCN**
TOTAL	**ML**	**4 8 286 340**	**32 4 820 696**	**24 4 657 135**	**35 6 078 580**	**21 3 028 717**	**16 1 192 072**	**7 351 049**	**139 28 414 592**
	FT								
	Other	**25 2 405 066**	**17 1 090 514**	**26 2 010 013 + 23 800 CZK**	**28 2 416 882 + 292 947 CZK**	**31 17 212 353 + 2 000 CZK**	**36 60 089 429 + 161,90957883 BTCN**	**18 19 182 236**	**181 104 406 495 + 161,90957 883 BTCN + CZK 318 747**
	Sum	**29 10 691 407**	**49 5 911 210**	**50 6 667 148 + 23 800 CZK**	**63 8 495 462 + 292 947 CZK**	**52 20 241 070 + 2 000 CZK**	**52 61 281 501 + 161,90957883 BTCN**	**25 19 533 285**	**320 132 821 087 + 161,90957 883 BTCN + 318 747 CZK**

291. The table above shows the performance of property related provisional measures regarding the seizure of bank account money. The authorities also provided further, more detailed statistics by breaking down the figures above according to the levels and branches of the Prosecution Service. While those additional tables are not shown here in entirety, their contents give room for some detailed analysis as follows (figures for 2019 are not considered in the conclusions below.)

292. Seizure of monetary funds pursuant to Art. 95 CCP took place most often in criminal investigations directed by County Prosecutor's Offices, both in ML cases and in general. At this level

of the Prosecution Service, such measures were used in ML cases with a remarkable frequency, as opposed to investigations into other criminal offences: the statistics show 105 seizures of funds for the entire period in ML cases, which is just as many as the occurrence of the same measure in all the other cases, partly because Art. 95 CCP is the measure by which funds previously frozen by FIU mechanism can be secured for the purposes of the criminal procedure. These funds were significantly higher in ML cases than in other proceedings (EUR9 536 496 in 105 cases vs. EUR6 422 246 in 106 cases). Similar tendencies can be seen in the figures for investigations directed by Regional Prosecutor's Offices, where 16 such measures were taken throughout the assessed period covering EUR15 366 871 as opposed to 23 seizures in non-ML cases covering only EUR1 024 860 and 25 800 CZK.

TABLE 31: Provisional measures taken by the Prosecution Offices according to Art. 95 of the CCP, broken down by type of Prosecution offices.

		2013	2014	2015	2016	2017	2018	Total
Seizure Regional PPOs	**ML**	1 8 275 024	2 2413 239	3 1 339 223	5 2 981 103	4 284 318	1 73 962	16 15 366 871
	Other	6 560 576		5 29 462 + 23800 CZK	6 177 499	4 216,175 + 2 000 CZK	2 41 145	23 1 024 860 + 25 800 CZK
Seizure County PPOs	**ML**	3 11 316	26 815 955	18 1 859 214	30 3 097 476	15 2 644 432	13 1108 101	105 9 536 496
	Other	12 585 506	15 580 514	17 1 583 739	19 2 070 382 + 292 947CZK	21 142 601	22 1 459 502	106 6 422 246 + 292 947 CZK
Seizure SPO	**ML**		1 10 000					1 10 000
	Other					1 15236 226		1 15 236 226

293. Another provisional measure the application of which is worth to analyse is the seizure of property pursuant to Art. 425 CCP (a measure applicable not only to concrete assets but to the entire property of the defendant). This measure was applied less frequently than the one in Art. 95 above, but the most important difference is that whereas seizure under Art. 95 was very rarely applied by the USP, the vast majority of the criminal investigations in which seizure under Art. 425 CCP was applied were led by the USP.

294. As shown by the excerpts below, such measure was applied 18 times in USP cases (out of which 2 ML cases) while 8 times in all cases dealt with by County and Regional Prosecutor's Offices. The total sum of assets secured by such measures was more than EUR22 million in USP cases (the ML cases representing EUR1 114 250) while all the other cases only covered EUR428 607. This reflects the type and severity of the more serious offences prosecuted by the USP (complex cases with high amount of proceeds, justifying the reinsurance under Art. 425 CCP where the entire property of the defendant can be seized for the purpose of future confiscation). In this context, the assessors note the sharp increase in USP seizures of bank account money in 2018 which covered the vast majority of such assets seized in that year.

TABLE 32: Provisional measures taken by the Prosecution Offices according to Art. 425 of the CCP, broken down by type of Prosecution offices.

		2013	2014	2015	2016	2017	2018	2019	TOTAL
Seizure USP	**ML**		1 1104250				1 10 000		2 1 114 250
	Other	1 100 000	1 10 000	1 45 000	3 169 000	2 1300000	8 19541 781	2 650 000	18 21 815 781
Seizure Regional PPOs	**ML**					1 932			1 932
	Other			2 293937		1 3469684	1 undefined value		4 328 633 84
Seizure County PPOs	**ML**					1 99 034	1 8		2 99 042 50
	Other								
TOTAL	**ML**		1 1104250			2 99 966	2 10,008		5 1 214 224
	Other	1 100 000	1 10 000	3 338937	3 169 000	3 1334696	9 19541 781	2 650 000	22 22 144 414
	Sum	1 100 000	2 1114250	3 338937	3 169 000	5 1434663	11 19551 789	2 650 000	27 23 358 639

295. As far as seizure of assets other than bank account money is concerned, the following table was provided to the assessors. Due to the difficulties with expressing the exact value of movable and immovable property that have been seized, the figures below are rather indicative.

TABLE 33: Summary of other seized property movable and immovable items + money other than in accounts

	Movable items		**Immovable items**		**TOTAL**
	description	**approx. EUR**	**description**	**approx. EUR**	
2013	KP	49 147	KP	710 000	
	OP	118 028 CZK 23 400	OP	0	
	ÚŠP	32,000	ÚŠP	268 000	
	Total	**199 176 CZK 23 400**	**Total**	**978 000**	**1 177 175 CZK 23 400**
2014	KP	525 116			
	OP	730 427 HUF 34 000			
	ÚŠP	1 302 502	ÚŠP not specified 1 104 450	900 000	
	Total	**2 558 045 HUF 34 000**	**Total ÚŠP not specified 1 104 450**	**900 000**	**4 562 495 HUF 34 000**
2015	KP	265 771		260 000	
	OP	304 351 USD6 CZK 516 540 GBP 85		90 510	

		HUF 1 336 000			
	ÚŠP	303 698		1 200 000	
	Total	**873 820 USD6 CZK 516,540 GBP 85 HUF 1 336 000**	**Total**	**1,550,510**	**2 424 330 USD6 CZK 516 540 GBP 85 HUF 1 336 000**
2016	KP	329 795			
	OP	533 745 CZK 3 135 USD1			
	ÚŠP	19 000		150 000	
	Total	**882 541 CZK 3 135 USD1**	**Total**	**150 000**	**1 032 541 CZK 3 135 USD1**
2017	KP	877 405		357 000	
	OP	275 862 HUF 8 000 CZK 74 000			
	ÚŠP	0	ÚŠP	1 500 000	
	Total	**1 153 267 275 861 HUF 8 000 CZK 74 000**	**Total**	**1 857 000**	**3 010 267 275 861 HUF 8 000 CZK 74 000**
2018	KP	472 947		374 000	
	OP	396 518 HUF 4 000			
	ÚŠP	21 688 781		37 000 000	
	Total	**22 558 247 HUF 4 000**	**Total**	**37 374 000**	**59 932 247 HUF 4 000**

296. While the cumulative table above appears to prove that LEA and prosecutors are capable of identifying and securing considerable amounts of both movable and immovable assets, a more thorough analysis gives room also for less positive conclusions. In general terms, the annual figures do not demonstrate any definite trends or tendencies – the amounts are increasing in the first part of the period then decreasing until 2018, in which year, however, an unprecedented increase was recorded. Here again, the Slovak authorities provided further, more detailed statistics as per levels and branches of the Prosecution Service, which show the following.

297. First, this sort of statistics (including both the cumulative table and the more detailed ones) does not contain some relevant pieces of information. It cannot be known, for example, which sort of provisional measure (which CCP provision) was applied for securing the assets indicated in the tables. It is unclear, how many criminal proceedings were involved and hence it is equally unclear in what proportion of the cases such measures were applied. Only the County Prosecutor's Offices statistics contained separated data for ML cases.

298. Aggregate figures show the following total amounts for the assessed period (2013-2018)

- USP cases: movable items in the value of EUR23 34 while immovable of EUR 41 018 000
- Regional PPO cases: EUR 2 520 183 + CZK 3 144 100 + ZL 36 660 + USD 6 517 (…) worth of movable while EUR 2 461 000 of immovable
- county PPO cases: movables in the value of EUR2 095 036 in ML cases and EUR 263 896 + CZK 550 475 + HUF 1 382 000 (…) in other cases, plus immovable in the value of EUR 42 700 and EUR 90 510 respectively.

299. Analysis of the more detailed statistics proves that the seized movables also included cash,

which appear to represent a considerable proportion of these assets, while the rest consists mainly of various vehicles, most of which must be physical instrument of a predicate offence, as well as various other items (firearms, computers, phones etc.). While the routine seizure of instrumentalities is thus adequately documented, the seizure of criminal proceeds should equally be demonstrable, for which reason the occurrence of cash, securities or similar property items in the movables and the figures for immovable assets were taken into consideration.

300. This segment of the statistics is, again, dominated by the USP results. Throughout the assessed period, 38 different real estates (flats, houses, lands) were seized in USP cases, with a sudden increase in 2018 when EUR 37 000 000 worth of immovable property was seized while, in the same year, an outstanding volume of funds and securities was seized also in USP cases (EUR 19 551 781). The assessors learnt that these figures stem from at least 4 major cases (mainly VAT fraud and related ML offences) where USP managed to secure at least EUR 15 million worth of assets, including various real estate in each case.

301. While these are commendable results indeed, they are also quite unprecedented as the figures for the previous years as well as for the first half of 2019 do not demonstrate any clear tendency or systemic increase in USP results, because of which these outstanding figures need to be reassessed in light of the results from the forthcoming years. As for the regional and county level Prosecutor's Offices, the results are not so significant, but they still demonstrate the ability of prosecutorial authorities at all levels (including 4 different Regional Prosecutor's Offices) to seize various immovable items and, specifically, their ability to seize significant amount of ML-related cash proceeds even at the lowest level of prosecution (EUR 2 095 036 seized in CPO cases).

302. Beyond the measures available in the criminal confiscation regime in Art. 58, 60 and 83 CC, the SR introduced other mechanisms to target ill-gotten assets. Deprivation of criminals of their illicit gains through civil procedure rather than criminal proceedings can be achieved by two separate systems within the Slovakian law. The first is the legal action for surrender of unjust enrichment on the basis of Art. 451 and further provisions of the Civil Code. Such a legal action can be brought by the prosecutor on behalf of the State pursuant to Art. 93 (1)a of the Code of Civil Procedure, claiming for unjust enrichment of a person so as to eliminate the effects of the unlawful disposal of property or by removing unlawfully acquired property. A prosecutorial action would be taken particularly in connection with criminal proceedings if it is not possible for the perpetrator of the crime, who obtained the property benefit, to impose a forfeiture of property, seizure of thing.

303. This measure was not at all applied until 2017. Since then, the prosecutors have submitted a total of 12 claims for unjust enrichment (3 cases in 2017 and 9 in 2019) covering a total value of EUR 98 714. Out of these, 7 claims have so far been successful, in which a total value of EUR 42 355 unjust enrichment has been lawfully granted to the State. While the frequency by which this measure is applied shows an obvious increase, the figures are still rather insignificant, particularly as the claimed sums are concerned. The AT has no information whether this measure has ever been applied in relation to criminal proceedings for ML offences.

304. Another non-conviction based measure is the action under the Act on Proof of Origin of Assets (No. 101/2010 Coll.) which was admittedly introduced as a remedy for the limits of the criminal confiscation regime (where the need for a conviction would usually place great demands on the law enforcement and prosecutorial authorities to bear the burden of proof), and the rather moderate results of other non-criminal measures such as the civil action for unjust enrichment (see above) or the administrative taxation proceedings. This measure is based on the assumption that everyone can prove the origin of their property and if this is not the case, the prosecutor

should have the right to initiate proceedings before a civil court on behalf of the State and require the defendant to rebut the well-founded doubts about the legitimate origin of their assets or else the court decides that such property falls to the State.

305. In such cases, the Financial Police Unit NAKA would first examine, either on the basis of a written notification or its own initiative, the income, value of property, and the manner of assets acquisition of a person, who they believe has acquired assets from illicit sources. Should the Police find, as a result of this examination, that the value of the actual assets of the investigated person has been higher by at least 1500 times of the minimum wage than his/her demonstrable incomes, the case is submitted to the prosecutor who may, after further investigation, file proceedings before the court related to acquisition of the property from illegal income.

306. Both law enforcement and prosecutorial authorities the AT met onsite admitted that the application of this measure raised various problems in practice and that the Act on Proof of Origin of Assets in its present form is basically inefficient. The search for the property is limited to the territory of the SR which excludes that any foreign assets can be considered. Furthermore, the value threshold being a precondition for the continuation of the proceedings, it is sufficient for the investigated person to dispose of just that part of their assets that exceeds the threshold of 1500 times the minimum wage, at any time after the initiation of the proceedings, so as to have the case dismissed. Practice shows that defendants would in such cases transfer their assets to third parties by providing fictitious gift contracts or fictitious credit and loan confirmations. Since the law allows that the investigated person may prove in any way the acquisition of the property, without the possibility of further investigation by the prosecutor or other authorities, this approach would automatically render all previous efforts of the authorities obsolete.

TABLE 34: Subject specification

Year	Subject specification - proving the origin of the property	Number of submissions
2013	24	0
2014	37	1
2015	37	0
2016	13	0
2017	9	0
2018	19	0
Total	**139**	**1**

307. Since 2011, when the said Act came into force, the Police have filed several complaints to the relevant prosecutors to initiate proceedings to declare that the property of a given individual was at least 1 500 times the minimum wage higher than the demonstrable income. Due to the shortcomings above, only one case was brought before the court in 2014 (involving property worth of EUR 130 346) but even in that case, the prosecutorial proposal had to be withdrawn as the evidential situation changed during the proceedings. The assessors were made aware of other cases, in which the defendant transmitted his property to his children or to companies where he served as a statutory representative, by which he succeeded to demonstrate, still in the examination stage of the proceedings, that his assets have decreased below the aforementioned threshold and thereby the procedure had to be terminated due to lack of assets.

308. No statistical figures regarding the amount of proceeds of crime returned to victims, shared or repatriated, were provided, hence, no general conclusions could be made in this respect. On the

other hand, Slovak authorities demonstrated by numerous case examples the applicability of the provisional measures and confiscation regime to secure criminal assets with a view to their repatriation as well as the practice by which such assets have regularly been returned to the victims. Repatriation of such assets has apparently taken place already during the stage of criminal investigations, by decision of the judge for pre-trial proceedings pursuant to Art. 95a CCP. Specifically, the assessors were provided with a range of ML case examples, in which proceeds derived from crimes committed abroad and then seized on Slovak bank accounts have routinely been returned to the victims in foreign countries.

309. It needs to note in this context, that Art. 50 CCP allows for the seizure of the defendant's assets (thus not the criminal proceeds themselves) for the purposes of victim compensation. Statistics provided in this respect show that this measure has been applied with a moderate frequency (18 cases throughout the entire period assessed, most of them prosecuted by the USP, out of which 5 ML cases) but the volume of secured property has recently increased, with 2 cases covering more than EUR 39 million in 2018 and 2 others covering more than EUR 18 million in the first half of 2019. By the time of the on-site visit, no final decision on victim compensation had been achieved in any of these cases.

310. There are some procedures, but no comprehensive mechanism for managing and/or disposing of property that is seized or confiscated. There is no centralized body in charge of management of such property, bearing a direct impact on effectiveness particularly if more complex types of assets have to be managed.

311. As far as seized property is concerned, general rules for safekeeping seized property items are provided for in the CCP as well as in the internal regulations No. 175/2010 and No. 7/2011 of the MoI (the latter dealing only with cars). In general terms, the secured monetary funds resulting from criminal activity are to be deposited on specific bank accounts of the MoI; precious metals and valuable items such as material securities, checks, bills of exchange etc. that require a particularly safe storage are to be kept in a safe deposit box provided by the General Credit Bank; seized items that require professional safekeeping (works of art, objects of archival and historical value etc.) is to be provided through another state body or legal entity or a natural person, which carries on business in that field, while motor vehicles, items of particularly large dimensions, are deposited by the Centre for security and technical activities of the MoI as the competent custodian for safekeeping.

312. These are clear and proper rules inasmuch as bank account money or tangible items are concerned, even if they require special care. There are however no specific rules for preserving the value by proper management of seized assets belonging to and being used by a business entity, either in the form of a real estate used for business purposes (*e.g.* a hotel, a ski resort, a farm etc.) and/or a set of movable items constituting accessories of a functioning business entity (*e.g.* equipment of a restaurant or a TV studio) where the mere custody or safekeeping of those assets would not compensate for the loss of value caused by the interruption of the business and could only be maintained by proper management (*i.e.* running the said business entities during the time when the assets are seized by the authorities). Another problematic area is the crypto-currencies, where the Slovak authorities demonstrated their capability to successfully seize and secure as well as to confiscate Bitcoins but the interlocutors met onsite were unsure exactly how the decision on

confiscation and thus the appropriation of the said crypto-currency would be executed[41].

313. The AT learnt that both the GPO and the Police had repeatedly proposed changes in the legislation governing the management of seized matters through the Ministry of Justice, upon which a draft law was repeatedly introduced to the Parliament but it was eventually rejected.

314. As far as factors that hinder the identification, tracing and confiscation of proceeds, the Slovakian authorities recurrently made reference to the absence of a central registry of bank accounts and, as a consequence, the length of time for processing applications from banks. Other obstacles mentioned by various LEAs were the burden of performing a financial investigation being put on the investigator responsible for the predicate offence (which basically refers to the Criminal Police but not the NAKA) resulting in an extra workload that prevents the investigator from carrying out a thorough and effective financial investigation. This, together with the generally time-consuming character of a financial investigation and the necessity to meet all procedural deadlines for the investigation of the predicate offence itself (particularly in custodial cases which need to be given priority) has a direct impact on the effectiveness. The deployment of 2 analysts to each regional Police Directorate is considered to solve this issue only partially and indirectly.

315. As mentioned above, the evidentiary standard required for the application of some provisional measures (particularly Art. 425 CCP on asset securing) that is, to prove there is a *"serious concern"* that the execution of a confiscation sanction will be wasted or hindered unless the provisional measure is taken, was reported to be interpreted by the courts in a way which practically renders this measure impossible.

316. Among further hindering factors, some of which was mentioned elsewhere under this Immediate Outcome, the authorities mentioned the (otherwise arguable) limits of seizing and confiscating assets from third parties, the improper legislation on the administration and management of seized property, the ineffectiveness of non-criminal mechanisms for confiscation, as well as the inability of LEAs to access specific databases and registers (ships, aircraft registration, etc.)

3.4.3. Confiscation of falsely or undeclared cross-border transaction of currency/BNI

317. The cross-border cash control regime, with and beyond its technical flaws regarding transport by mail and cargo, has not demonstrated its effective applicability to detect ML/TF related cash/BNIs transported through the borders of the Slovak Republic that also constitute external borders of the EU (these being the eastern border with Ukraine as well as the international airports in Bratislava, Poprad and Košice). The cross-border cash control is to be dealt with exclusively by the Financial Administration (Customs).

318. Technically speaking, the measures to detect illegal physical transport of cash/BNIs are present at the external borders. The control would be performed by Customs authorities based on the application of risk analysis by targeted selection of persons representing the risk, determined by the experience of customs officials in the field of smuggling detection and assisted by technical means including X-ray screening or cash-seeking service dogs. In case of suspicion, the individual is subjected to a security inspection and, in a justified case, also to a personal search including the examination of body cavities.

---

[41] Subsequent to the onsite visit, the Slovakian authorities found a solution for this problem. A hardware Bitcoin wallet was established at the district office (the state authority responsible for disposal of forfeited property) with the assistance of the Cybercrime Police Department, to which forfeited Bitcoins can be transferred for further disposal.

319. Notwithstanding all these, the actual results are rather poor, both in general terms and in relation to cash/BNIs either derived from criminal activities or intended for TF. The table below summarizes the incoming/outgoing declarations as well as the few cases of false or non-declaration of cash/BNIs that have occurred throughout the assessed period.

Table 35: Cross border transportation of currency and bearer negotiable instruments

Year	Number of declarations or disclosures				Suspicious cross border incidents	
	Incoming		Outgoing			
	Currency	BNI	Currency	BNI	BNI	False declarations
2014	55 EUR 1 609 716	0	4 EUR 142 998	0	0	2 EUR 41 836
2015	70 EUR 2 737 054	0	3 EUR 154 817	0	0	0
2016	121 EUR 3 956 678	1 USD 25 000 000	3 EUR 59 769	0	0	7 EUR 127 010
2017	146 EUR 5 035 417	1 USD 14 975 000 000	6 EUR 225 998	0	0	16 EUR 435 371
2018	221 EUR 7 811 560	0	9 EUR 320 265	0	0	23 EUR 344 120

320. The number of incoming currency declarations is remarkably high with generally modest aggregate sums, which appears to confirm the Customs opinion that in most cases, the purpose of cash transport is mainly to acquire movable property (such as motor vehicles) or real estate. The number of outgoing declarations is just a fracture of those incoming, even if the average sums appear to be higher in these cases. More detailed statistical information provided to the AT proves that the majority of incoming declarations were made at border control points (BCPs) with Ukraine (although the number and volume of currency declared at international airports shows a significant increase) while the outgoing declarations were rather balanced in this respect.

321. The Customs authorities opined that the presumable purpose of incoming cash transportation (purchase of vehicles or real estate) would in itself demonstrate that such forms of cross-border cash transport represents a low risk of ML/TF. Considering, however, that transforming of illicit money into property items (and particularly real estate) may easily constitute a form of ML, the AT has concerns regarding this argument.

322. Lack of sufficient ML/TF risk awareness can be illustrated by the 2 occurrences of declared physical transport of BNIs as indicated in the table, that is, one occasion in 2016 where USD25 000 000 worth of BNIs were carried into Slovakia and another one in 2017, where the value of BNIs involved (as it was confirmed by the Slovak authorities) was of USD14 975 000 000. The AT learnt that both transports (2016 and 2017) took place and thus were declared at the Bratislava Airport and both were performed by the very same Czech citizen. The authorities explained that the BNIs had originally been issued in the USA then sent by ordinary mail to Hong Kong before being acquired by this Czech citizen who declared he wanted to use them as investment into an aviation company in Slovakia. Despite the obviously suspicious circumstances (*e.g.* that the nominal value of the 2017 BNIs was 17,7% of the Slovakian GDP for the same year[42]) the Customs authorities accepted this statement in both cases and let the person enter Slovakia with the BNIs without any further investigation. When the FIU was informed of the first transport and declaration in 2016, they notified the Czech FIU (no information about any further action in 2017)

[42] Source: statdat.statistics.sk

and requested information from their USA counterpart with no response. It is unclear if the FIU or any other Slovakian authority proceeded to examine the background of the person and his purported investment and whether the cooperation with the Czech authorities did yielded any results.

323. The AT has similarly serious concerns regarding those cases where the rules applicable for the cross-border transport of cash/NBIs have actually been violated through non-declaration or submitting a false declaration. These cases were related, without exception, to incoming transports and were practically limited to one of the land border crossing points with Ukraine and the Bratislava Airport. First, the Customs appear to have detected an alarmingly low number of such cases (48 instances throughout the entire assessment period) involving relatively moderate sums of money. Second, as it was confirmed onsite, in neither of these cases have any assets been restrained by the authorities and therefore no further provisional or confiscation measures could be applied. Third and last, the authorities detected zero cases where the transport of cash/BNI raised any suspicion of ML or TF activities which, in light of the aforementioned technical background to identify such cases, calls for some explanation.

324. Failure to report or submitting a false report is considered a customs offence, which is resolved by the Customs authorities pursuant to the Customs Act (199/2004, Coll.). In case a criminal offence is suspected in connection with such transport, the appropriate unit to carry out the proceedings would be the FDSR in relation to crimes committed in connection with the violation of VAT legislation on import and excise duties, while the competent Police department in case of any other criminal offences including ML/TF. Notwithstanding that, no criminal offence has so far been detected in such cases and therefore this repressive mechanism has not yet been used in practice. It needs to note in this context, that even if border police officers are present at the border crossing points, they do not cooperate to any extent with Customs officers as far as the control of the movement of goods (including cash/BNIs) across the state border is concerned.

325. The AT noted as a further shortcoming that there is no mechanism available to counter cash couriers entering through the EU internal borders (namely from Poland, the Czech Republic, Austria or Hungary).

3.4.4. Consistency of confiscation results with ML/TF risks and national AML/CFT policies and priorities

326. As discussed in IO.1 above, the main ML threats indicated in the NRA were the criminal offences against property (theft, fraud) the economic crimes in general (particularly tax crimes) and the so-called *"specific partial types of crime"* covering organized criminality, drug-related crimes, cybercrime and corruption. According to the Slovak authorities, forfeiture/confiscation measures are indeed applied mostly for property and economics crimes while only moderately for other sorts of criminality, although positive tendencies were mentioned in this field in line with the development of more effective forms of financial investigations.

327. Unfortunately, this could only to a very limited extent be verified by statistical data as the AT were not given any meaningful information as to what criminal offences have been represented in the statistics on the performance of the confiscation and provisional measures regime. There was a general and absolute lack of information regarding the confiscations while only partial figures were provided in the area of the provisional measures (*e.g.* for statistical tables relating to USP cases) which were too fragmented to draw any conclusion. In any case, the numerous case examples provided by the authorities to illustrate the performance of the confiscation regime were dominated by economic and property crimes (and related ML) although some significant drug and

OC related cases were also mentioned.

328. The main ML vulnerability identified in the NRA with a direct impact on the confiscation and provisional regime was the lack of specialization in identifying and tracing of criminal proceeds and in performing financial investigations which resulted in insufficient level of seizure and confiscation. As it was discussed under IO.1 the AT gives credit to the GPO for having recognized shortcomings in this area and for their efforts in the field of policy making and issuing methodological guidance to the practitioners. Some increases in specialized LEA staff were also mentioned above. Due to the recent nature of most of these measures, however, the results are likely to be seen in the forthcoming years.

329. As a result, the AT could not establish whether confiscation results were consistent with ML/TF risks identified and that the performance of the entire confiscation regime (that is, beyond the initiation of financial investigations and applying provisional measures) was in line with national AML/CFT policies and priorities.

Overall conclusions on IO.8

330. Although a range of robust legal instruments are available for the Slovak authorities to seize and confiscate proceeds and instrumentalities of crime, the effective application of these measures is highly unbalanced. Provisional measures are regularly and systematically pursued by law enforcement and prosecutorial authorities in the course of financial investigations, the frequent use of which, however, does not appear to be followed by the confiscation regime. Forfeiture/confiscation measures are rarely applied, and therefore only a fragment of the secured assets will finally be confiscated. On the other hand, the effectiveness of the provisional measures is seriously affected by a series of hindering factors such as the lack of proceeds-oriented operative analysis in the pre-investigative proceedings, the logistical and procedural constraints at certain LEAs or the high evidentiary burden required for certain provisional measures. There are some procedures, but not a comprehensive mechanism for the managing and/or disposing of property that is seized or confiscated and neither is there any centralized body in charge of management of such property. The cross-border cash control regime has generally failed to demonstrate its effective applicability to detect ML/TF related cash/BNIs transported through the borders of the Slovak Republic.

331. **Overall, the Slovak Republic has achieved a Low level of effectiveness with Immediate Outcome 8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

4.1. Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

1. Since the previous evaluation, the criminalization of TF has developed due to the introduction of a more comprehensive, stand-alone TF offence in 2018, together with other provisions completing the range of underlying terrorism-related offences (including Art. 419d on foreign terrorist fighters).

2. The NRA identifies the TF risk in Slovakia as low due to several factors such as country's geographical location, its population profile and its economy. However, the assessors identified some shortcomings in relation to the accuracy and completeness of the NRA, with some potential TF risks not being fully addressed. (*e.g.* poor control on the cash movements across the country; money remittances, the use of fictitious corporate structures; non-dissuasive nature of sanctions in relation to undeclared/falsely declared movement of cash etc.).

3. There have been no TF convictions in the assessed period. Three relatively complex TF investigations are currently conducted by the CTU - NAKA. The TF investigations introduced to the assessors demonstrate both the applicability of the legal framework and the ability of the Slovak authorities to effectively cooperate with their foreign counterparts. It is to be noted, however, that despite the length of the procedures, no charges have yet been pressed in any of these cases and, as a consequence, no terrorism-related funds were restrained either.

4. The FIU filters some 20% of the TF UTRs, the rest being disseminated to LEA. In the assessed period, a total of 464 UTRs have been sent by the FIU to the responsible LEA Unit, namely the Fight Against Terrorism Unit of the Police Force Presidium (until 2016) and CTU – NAKA (after 2016). The FT related UTRs are simultaneously sent to SIS.

5. TF investigations are partially integrated with the national strategies at the operational level due to strong inter agency collaboration and the existence of formal working groups. TF elements are not sufficiently reflected in national counter-terrorism action plan (CT-NAP) 2016-2018 which is focused on terrorism.

6. The CTU - NAKA investigators seem to have the necessary skills and knowledge to identify and investigate FT if needed. On a less positive side, no particular measures have been taken to increase awareness and knowledge of other LEA and Prosecution on TF risks, typologies and effective use of financial intelligence to conduct investigations.

Immediate Outcome 10

1. The designation procedure involves a number of responsible state bodies. The MFA has the clear role to communicate the potential proposals to UN Committees. However, there are no clear regulatory instructions defining a leading competent body for designations. To date, the Slovak Republic has not proposed or made any designations.

2. The shortcomings identified in the EU legislation resulting in delays of implementation of targeted financial sanctions pursuant to UNSCRs 1267/1989 and 1998 impact the application of TFS in Slovakia. To address these deficiencies, the authorities introduced a national mechanism which provides the direct legal effect of the decisions taken by the UNSC Committees and related

regulation. No assets have been frozen pursuant to UNSCRs which is in line with the country profile.

3. Most of the financial sector have a good understanding of their freezing and reporting obligations. FIs mostly use commercial databases or have developed their own automated screening systems to check clients and to update the sanctions lists. The understanding of TF TFS is uneven across DNFBPs, with auditors having a fairly good knowledge on their obligations, while the lawyers, accountants and the dealers of precious metals and stones lack sufficient awareness on the matter.

4. The NRA sees the NPOs' exposure to FT abuse as low, but no specific types of more vulnerable NPOs have been identified. SIS and CTU -NAKA perform supervision over a certain number of NPOs, but this appears to be done more on a cases-by-case basis rather than systematically.

5. There is no specific risk-based outreach for NPOs concerning their potential misuse for TF purposes but the NPOs seem aware of the risk due to big donors' regulations.

6. The NPOs have an obligation to open a bank account and to send annual activity reports containing statutory information. Prior to the registration with the Registry Office, the statutory body of the NPOs must prove integrity by absence of criminal records.

Immediate Outcome 11

1. The PF TFS in Slovakia follows the EU mechanism which displays certain elements of an effective system. At national level, the ISA applies as in the case of TF TFS.

2. No funds related to PF have been frozen in Slovakia, which is in line with the country's risk profile;

3. The MFA webpage refers to the main page of the UNSC which subsequently redirects to consolidated version of sanctions lists. The lists are available and accurate, and there is a mechanism to notify the changes occurred at EU level to the competent state authorities.

4. The level of understanding of PF-related TFS obligations among larger financial institutions is sufficient and they rely on commercial databases to identify matches with sanctions lists. Other REs have a more limited awareness on the PF sanctions and at best perform manual checks on their clients when certain suspicions occur. Non-banking REs have difficulties to detect funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities.

5. Supervision on implementation of TFS forms a part of inspections conducted in relation to banks by the NBS, although there is no supervisory risk model that would include issues on the implementation of UN TFS related to PF. Supervision over the DNFBPs on PF matters is inadequate.

6. Although the MoF developed a guidance on procedures for implementation of the UNSCRs by the financial institutions, limited training on implementation of TFS has been provided to the RE. No guidance was developed for other types of obliged entities.

Recommended Actions

Immediate Outcome 9

1. Financial investigations should be carried out more proactively and effectively in all terrorism and other cases from the early stages and without delays, including through systematically accessing FIU TF related financial information.

2. GPO would benefit from having a TF specific strategic approach establishing goals such as timely TF investigations using all available tools including financial analysis to more effectively finalise the TF case.

3. The authorities should take measures to ensure that the operational (pre-investigative) phase is not open-ended and establish clear formal rules on which a pre-trial TF investigation is undertaken, ensuring an effective monitoring of the results of the operational phase.

4. Internal and external border cash control mechanisms should be strengthened by providing a legal basis for the possibility to stop and restrain terrorism and FT suspects assets administratively, and to support the identification of such assets by continuing developing typologies and indicators.

5. The CTU - NAKA and GPO should benefit from more training on TF investigations and prosecutors including international case studies of successful terrorism financing investigations.

Immediate Outcome 10

Slovakia should:

1. Streamline the designation mechanism with clear responsibilities for one or more authorities and precise instances when the designation should be made and by whom. Alternatively, a single dedicated specialised authority with a leading role in the implementation of TF TFS should be appointed.

2. Provide adequate training on implementation of FT TFS for the all REs, with special focus on DNFPB sector.

3. Revise or conduct a new in-depth risk assessment of the NPO sector to identify categories that are at risk of the FT abuse. Adopt a targeted, coordinated, RBA to oversight of higher risk NPOs, including outreach and awareness raising for NPOs and the donor community, with a focus on end use of NPO funds.

4. Take measures to enhance authorities' awareness on the application of the EU Regulations, including when divergent from the national legislation.

Immediate Outcome 11

1. Authorities should engage in PF TFS awareness raising actions and provide guidance, especially in relation to the non-banking REs and DNFBPs.

2. The NBS's should include implementation of PF TFS in its supervisory risk model.

3. Designate a supervisor for the DNFBPs responsible for monitoring the implementation of PF TFS by the DNFBPs.

332. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The Recommendations relevant for the assessment of effectiveness under this section are R. 1, 4, 5–8, 30, 31 and 39.

4.2 Immediate Outcome 9 (TF investigation and prosecution)

333. The issue of financing terrorism and terrorist offences is comprehensively regulated by the provisions of the CC (see the TCA).

334. The NRA concludes that the TF risk in Slovakia is medium-low due to several factors such as country's geographical location, its population profile and its economy. The assessors identified

some shortcomings in relation to the accuracy and completeness of the NRA (see Chapter 1 and IO1), and considering the content of the on-going TF investigations, the AT is reluctant in considering this assessment as fully accurate. No convictions have been pronounced by Courts for TF or terrorism offences.

335. The key players within the CFT framework are the CTU - NAKA, the FIU, Slovak Information Service (SIS), Military Intelligence and the Special Prosecutor Office of the General Prosecutor's Office (SPO).

336. The SPO has a special role in this area, covering all offences of terrorism under the CC, *i.e.* acts committed with the intention of committing a terrorist offence, as well as the offence of establishing and supporting a terrorist group. All these terrorist offences are dealt with by the Specialized Criminal Court in the first instance, and the Supreme Court of the Slovak Republic acts on any possible appeals against his decisions. Currently SPO has five prosecutors dedicated for supervision and prosecution of terrorist offences.

4.2.1. Prosecution/conviction of types of TF activity consistent with the country's risk-profile

337. While there have been no TF convictions in Slovakia so far, this is largely consistent with its risk profile. Nevertheless, there are three relatively complex on-going TF criminal investigations conducted by the CTU – NAKA under prosecutor's supervision. The specifics of the TF investigations, as introduced to the assessors, appear to demonstrate both the applicability of the legal framework and the ability of the Slovak authorities to effectively cooperate with their foreign counterparts. It is to be noted, however, that despite lengthy of the procedures, no charges have yet been pressed in any of these cases and, as a consequence, no terrorism-related funds have been restrained either.

338. The TF cases are prioritized by the relevant LEA, and a special approach is applied by prosecutors of SPO in TF cases, as in the course of the investigative procedure, there is a systematic supervision of the case, and instructions are given to the Police officer in charge. The prosecutors also personally ensure the coordination with the foreign counter-parts.

339. It is difficult to conclude whether the results achieved in the period under review are fully consistent with the country's risk profile in the absence of final decisions in the existing cases. The AT has no reason to believe that the mechanism in place to prosecute and convict persons for FT would not work effectively, however, a considerable amount of time elapsed since the initiation of the proceedings (at least in two of the three cases), which raises concerns. The prosecutors should be more pro-active when supervising the early stages of the TF investigations and put more pressure on the police officers to timely gather evidence and move the case into the next step of the criminal procedure, either by pressing charges or by closing the case.

340. Whereas the TF risk is *"medium-low"*, a more granular analysis is needed in the new iteration of the NRA, which should take into account the features of the on-going TF cases, in which Slovakian citizens and/or residents are suspected of being involved. In two of the three investigations Slovakian financial institutions appears to have been used.

4.2.2. TF identification and investigation

341. As a rule, the CTU – NAKA would investigate all TF cases with input from FIU and other bodies, out of which the SIS stands out. The SIS would not carry out investigations by themselves, but they would collect information on terrorism, TF and terrorism propaganda. They survey the sensitive communities, target persons, and financial transactions. SIS information is provided to the CTU – NAKA to add or to complete some investigations, but the nature of such was not disclosed to the AT.

342. The AT thoroughly looked at the statistics presented by the Slovak authorities on the number of TF related UTR[43] disseminated by the FIU to LEA, which were not followed by the initiation of a criminal investigation, all being stopped at operational level. The one investigation started on the basis of an FIU dissemination was not UTR based but emerged from an international information request from a third country.

343. As in case of ML suspicions, the FIU enriches the UTRs with all available information and sends the results to the CTU – NAKA and SIS. Some 20% of the total number of TF related UTRs are filtered at FIU level as not baring sufficient suspicion elements. For the description of the analysis performed on UTRs, the reader is referred to *"operational analysis"* sub-chapter under IO6.3.

344. In turn, the CTU – NAKA states that every single FIU dissemination becomes subject of an operational investigation which includes a preliminary financial analysis, as it does for any other disclosures. The information is checked against all available information: the police databases; international databases (Europol, Interpol); open sources (Companies Register, Trade Register, Real Estate Register, etc.). In case deeper checks are needed, on-site verifications are conducted by NAKA police officers. In the process of preliminary FT investigations, intense information exchange with all relevant domestic counterparts is taking place (*i.e.* FIU for international information requests). In some instances, this exchange is supported with NSAC capacities.

345. There was one TF criminal investigation started by LEA based on FIU dissemination, which was not UTR based (see Case B below). For the rest of the disseminations the authorities explained that after thorough consideration, it was concluded that the UTRs contained un-founded partial matches with Worldcheck names or sanctions lists (other than UN TFS or PF lists) or, in other cases, remote links with high risk third countries (funds transferred or received from such countries, client or statutory body from those countries, etc…). Hence, the cases were closed.

346. For every FIU dissemination, the CTU – NAKA sends feedback to the FIU on the action taken and the final decision adopted, which so far was limited to storage in the system for further needs. Despite the above feedback, the AT has doubts about the effective coordination and communication between the CTU – NAKA and the FIU, since the disseminations continue to be sent without results in terms of investigations.

347. GPO SPO are not formally involved in the operational phase of a TF case if the LEA does not open a formal criminal investigation. Therefore, as already expressed under IO7, there is no independent legal authority who can review the decisions of CTU NAKA when a case is stopped at the operational level. Authorities (LEA, GPO) should formalize, review and verify the decisions of LEA not to initiate criminal proceedings in the TF identification phase.

348. The SIS double checks the FIU disseminations and contributes to potential TF cases if need be. Their experience confirms the lack of TF elements contained so far in the UTRs. In one case, following a FIU information, SIS analysed the transactions of one person having transferred funds abroad to a natural person linked to perpetrators of a terrorist attack. A thorough inquiry having been carried out, including through the international cooperation, a financial support to terrorism was ruled out in this case.

349. The SIS is involved in several international platforms dealing, among other issues, with the TF. An operational information sharing is performed through secure communication channels. Any suspicious operations could be compared with findings of partner intelligence services, this being important especially with regard to the international nature of TF.

---

[43] In the assessed period, a total of 464 UTRs have been disseminated to the Unit of the Fight Against Terrorism of the Police Force Presidium (until 2016) and Counter-Terrorism Unit – NAKA (80 in 2013, 79 in 2014, 83 in 2015, 93 in 2016, 69 in 2017 and 60 in 2018).

350. The prosecutors confirmed that the CTU – NAKA is pro-active in initiating a significant number of operative actions even in case of a very low suspicion threshold and leaves no stone unturned in potential TF cases. The AT has no reasons to disbelieve this statement.

CASE BOX 12: The "Imam case" – Case A[44]

The case was initiated by the CTU – NAKA in July 2017, based on an international information request received from a foreign jurisdiction. In fact, a religious leader (Imam) collected money from the believers (between 2015 and 2017) in praying rooms (the authorities explained that there are no mosques in Slovakia) for *"buying water pumps in a poor country"*. The money was collected not only in Slovakia but also in the Czech Republic. In the course of the investigation it was established that the donations were collected in cash and subsequently deposited in two bank accounts, transferred to the Czech Republic and then to Syria to support terrorists or terrorist groups. The Czech authorities issued the first arrest warrant and extradited the Imam. The investigations made by the Slovak authorities were extended to the persons (approximately 60) who were identified as having provided donations. All of them were interviewed and the prosecutors concluded that they were not aware of the actual destination of the funds. During the investigation, the Slovak authorities were able to identify one person – Mohammed H., who contribute to collections of money and later travelled with money to Syria. He joined a terrorist group called *"Jabhat Fatah al-Sham"* or *"Al-Nusra Front"* and participated on its activities. Mohamed H. was "killed in action" in a late 2018. At the time of the on-site interviews the case was on-going.

No provisional measures have been taken in this case, as the Imam did not possess any assets on the territory of Slovakia.

351. The TF cases investigated so far have been triggered by three different sources: one as a result of a LEA international cooperation (case A), one based on FIU international cooperation (case B) and the third emerged as a new suspicion in the already existing case investigated for another crime (case C). With the exception of Case A above, the AT and the assessed country decided not to present the other two individually in case boxes, but to briefly describe them in the paragraph below.

352. Case A included some financial investigations although rather rudimentary as most of the monetary transactions have been done in cash. The AT deplores the lengthy procedures in Case A. Case B involved money remitting services and UTRs but with a strong input from a foreign counter-part. A relatively high number of countries and individuals are involved in Case B and while the measures at FIU level were swiftly taken, the procedure at the LEA level is tedious, lasting for more than 2 years. In this particular case, the authorities maintained that the lengthy procedures were generated by the absence of reply to several MLA requests which blocked the advancement of the procedures. Case C was initiated just before the on-site visit in the context of a complex investigation related to other (serious) crimes. Amongst other measures, financial operations conducted through financial institutions are subject to investigations into possible TF.

353. As a rule, the financial investigations are performed by police officers and rarely by the prosecutors themselves, although it was clear that there is no legal impediment to doing so if need be. The prosecutors acknowledge that there is room for improvement in this respect, especially by providing training to the police officers or having access to specialized experts.

44 After the on-site visit, the Slovak authorities reported progress on the case, the person charged in the Czech Republic being convicted for terrorism and TF. The authorities expect the application of ne bis in idem principle.

354. The three cases, as well as the on-site interviews, demonstrate that the Slovak authorities are prepared to identify a TF case from various sources and to take the necessary investigative measures including by exploring the financial side. On financial investigations, there is progress from LEA side: while Case A included a rather simplistic financial analysis, the other two appear to be handled in a more comprehensive manner, as they include bank accounts and legal entities. For this progress the Slovak authorities should be commended. Nevertheless, tangible results in terms of convictions and assets restrained cannot be reported.

355. There is an obvious lack a specialization both on financial analysis and on TF typologies more generally. The LEA and Prosecutors encounter challenges in: i) producing sufficient evidence on the TF related financial trails ii) proving the mental TF element. This results in important delays in finalizing the TF cases and bringing the culprits to justice in a more effective way. The assessors reiterate the concerns regarding the lack of regulation and insufficient supervision over the operational phase of the investigative process (see IO7).

356. Turning to the TF risks related to the cash movement, as described under R32, the Customs do not have the specific power to stop and restrain currency at the borders in order to ascertain whether evidence of TF may be found. This was confirmed by authorities met on-site. This raises some concerns about the ability of the authorities to identify and initiate TF enquiries at the borders.

357. To address the above and the deficiencies identified in NRA process, at MISO-LP CFT sub-group an interdepartmental exercise was organized in February 2018 under the umbrella of the MoI. The purpose was to train the competent units of the Police Force and other involved entities on the detection and investigation of terrorist financing. The topics of the training were related to successful identification of suspicious transactions, implementation of adequate preventive instruments, and better understanding of potential TF methods and trends.

4.2.3. TF investigation integrated with – and supportive of - national strategies

358. Slovakia's TF investigations are partially integrated with the national strategies as reflected in the AP 2019, but the TF elements are not clearly reflected in the CT-NAP 2016-2018. These conclusions are based on a review of the CT-NAP, AP 2019 and discussions with the LEAs, prosecutors, FIU and members of the MEKO.

359. The MoI regularly prepares and up-dates (every 4 years) the CT-NAP, a strategic document, with the purpose of creating a suitable environment for the completion of international commitments, such as bilateral and multilateral agreements, resolutions of UNSC, decisions and resolutions of EU institutions or sanctions of international institutions against persons and entities related to terrorism. The CT-NAP contains a summary of the main tasks in the fight against terrorism, including the fight against terrorist financing, addressed to the competent national authorities, which should fulfill them within specified deadlines. The implementation of the tasks is continuously monitored by the Ministry in charge of each action and the NAP itself is evaluated after the end of the period.

360. The CT-NAP 2015-2018 include the following tasks related to the fight against terrorism: i) increase the expertise and qualifications of the employees involved in counter-terrorism; ii) conduct the training activities for staff of participating ministries to raise awareness in the field of extremism and terrorism; and iii) educate members of the Police Corps, members of SIS dealing with the fight against terrorism, focusing on the development of security risks, terrorist trends and means of their effective elimination. The up-dated CT-NAP entered into force after the on-site visit.

361. Turning to the AP 2019, although some relevant TF risk mitigation measures have been included in the list of actions to be taken to increase effectiveness of TF investigations, little measures have been taken in practice due to the recent adoption of the said document.

362. While the authorities appeared to be conscious of the importance of deterring the TF and do prioritize the (few) existing cases, there is a lack of practical experience and training in investigating of this type of crime. More resources need to be allocated for training, technical and software equipment, at a minimum for the CTU – NAKA and the FIU.

363. The internal cooperation and coordination on TF matters is satisfactory. Operative issues are discussed at the NSAC, an interdepartmental organizational structure in the form of a joint workplace, bringing together the national authorities involved in the field of combating TF and other serious security threats. The key tasks of NSAC are the preparation of comprehensive analytical assessments of security incidents based on reports and statements received from state authorities, monitoring security situation in open sources, and the provision of analytical products on security threats to designated recipients. Representatives of NSAC meet on daily bases. All members have access to the NSAC information system and share state security relevant information.

364. To ensure an effective way of operational information exchange and in order to avoid duplicative activities in solving individual ML and TF cases, a TF dedicated sub-group NES-FT sub-group was established within the MEKO.

4.2.4. Effectiveness, proportionality and dissuasiveness of sanctions

365. The Slovak legal framework provides for a dissuasive sanctioning regime for TF crimes (see analysis under R5). Nevertheless, in the absence of convictions, the practical implementation of the sanctioning regime effectively and proportionally cannot be assessed. It can only be stated that the meetings with the judiciary indicated that the seriousness of the TF crime is well understood, and that appropriate consideration would be given in the judgment of the sentence if the case arise.

4.2.5. Alternative measures used where TF conviction is not possible (e.g. disruption)

366. The authorities have never applied alternative measures in lieu of proceeding with FT charges.

Overall conclusions on IO.9

367. Slovakia has no TF prosecutions or convictions which is largely in line with the country risk profile. There are three on-going criminal investigations carried out by LEA under SPO's supervision. In one case delays in finalizing the investigation were noted. At operational level, which includes a preliminary financial analysis, the CTU – NAKA looks into every single FIU dissemination, as it does for any other disclosures. The operational phase appears to be too lengthy and needs an effective monitoring. Slovakia's TF investigations are partially integrated with the national strategies. There is an intense information exchange among all relevant domestic and foreign counterparts on FT investigations. In the absence of convictions, the practical implementation of the sanctioning regime cannot be assessed, but the judiciary appears to understand the seriousness of the TF crime.

368. **Slovakia is rated as having a Moderate level of effectiveness for IO.9.**

4.3. Immediate Outcome 10 (TF preventive measures and financial sanctions)

4.3.1. Implementation of targeted financial sanctions for TF without delay

369. As a member of the EU, Slovak Republic applies the EU legislation for the implementation of TFS. The EU framework does not provide the possibility to implement the TFs *"without delay"* as far as deficiencies in timely transposition of UN designations into the EU legal framework exists.

370. At the national level, the International Sanctions Act (ISA) creates a system for the *"Autonomous Declaration of International Sanctions"* (Art.3) according to which the government of the Slovak Republic shall declare an international sanction by Ordinance. This system is applicable to designations pursuant to UNSCR 1373, UNSCR 1267/1989 and 1988.

371. According to the ISA, the MFA is the authority responsible for submitting a designation request to the relevant UNSC Committees through the Permanent Representation to the UN.

372. The ISA establishes a designation procedure, which makes reference to a *"responsible authority"* which can be any state body in Slovakia[45]. The competent authorities with the capacity to investigate into a suspicion of an individual or entity falling within the frame of the ISA are all the ministries and administration authorities of the Slovak Republic. If a ministry looks at a case and deems it has no competence over it, shall immediately pass the motion to the responsible ministry. According to the authorities, this wide range of competent bodies is following the structure and the competences of the state authorities in the country.

373. During the on-site visit, the AT met a wide range of potential *"responsible authorities"* who were not able to clarify who will make the proposal and in which circumstances should the case occur. This raises concerns, as it appears that in the absence of clear regulatory instructions, the authorities may rely on each other to make the designations, which may result in overlooking a potential case even if the persons or entities would meet the designation criteria. Although the MFA is the well set *"communication"* channel with UN, it does not assume itself as the competent leading body specialized in this regard.

374. The next step in the designation process is the consultation stage, where the MoF, the MFA, the MoI, the Ministry of Defence, SIS, and the Military Intelligence, must be requested by the designating body, to give their opinion on the proposed persons or entities. Should any of those authorities oppose to the designation, the proposing authority shall suspend the proceedings. Other state bodies may be invited to such consultations.

375. The *"consultations"* mechanism has never been tested in practice. The whole designation process is limited to maximum of 30 days from the initiation of the proceeding, which is reasonable delay. If the facts justifying the suspicion in accordance with the ISA have been sufficiently demonstrated, the designation is made, otherwise the proceeding shall be suspended.

376. The MFA serves as the entry point for receiving designation requests from third countries. If a third country request is received, the MFA forwards this request to the relevant state authority for its consideration to launch the inter-agency consultative process as described above. In this process, the MFA submits its official position considering Slovak foreign policy interests to the relevant state authority to make a decision on the third country request.

---

[45] The NAKA, the Financial Administration Criminal Office, the Military Intelligence, the Office of Criminal Police, the FIU, the MoF, the MoI, the MoD, the MoJ, the MFA, the Ministry of Transport, the Ministry of Labour, the Ministry of Environment, the Ministry of Education, the Ministry of Culture, the Ministry of Soil Management, the Ministry of Health Care, the Ministry of Construction.

377. To date, the Slovak Republic has not received requests, proposed or made any designations pursuant to UNSCRs 1267 and 1373.

378. Turning to the communication of UNSCRs lists, Slovakia has a two folded notification system. On one hand, designations under the UN and EU are communicated to the REs and the public by posting the sanctions lists on the MFA website. In addition, when the lists are up-dated, the MFA immediately sends electronic notifications to the domestic relevant bodies, to draw attention on the changes. Links to both consolidated UN sanctions lists are published on the MFA website.

379. Shortly before the on-site visit, the MoF issued the *"TFS Procedures"*, to instruct the entities in the financial market in identifying individuals, transactions or assets which are subject to international sanctions. The *"TFS Procedures"* details the reporting duties and provides guidelines on how the REs should act in case of a *"hit"* depending on the sector, financial product and sector profile (transactions, loans, securities, life and non-life insurance).

380. Most of the financial sector have a good understanding of their freezing and reporting obligations. FIs mostly use commercial databases or have developed their own integrated screening systems to check clients and to automatically update the sanction lists. Clients are checked against the TFS lists when establishing the business relationship, and in every occasion when transactions are carried out. Regular checks of client database are automatically performed by banks.

381. Understanding of obligations and responsibilities related to implementation of the TF TFS varies across DNFBPs which rely on the publicly available information from the MFA website. The checks are done manually. While the notaries and auditors are better informed about the TF sanctioning regime, the lawyers, real estate agents and the casinos seem to lack sufficient awareness regarding their obligations and do not conduct checks against the TF designation lists on their clients. Nevertheless, those sectors are less significant from the materiality point of view (see Chapter 1).

382. The private sector is unanimous in saying that the competent authorities could provide more outreach in this field. While welcome, the adoption of the *"TFS Procedures"* had a moderate impact on the REs due to limited trainings and awareness raising programs undertaken subsequently by the authorities. In practice, the REs continue to rely on their own self-developed procedures and regular internal trainings to their employees.

4.3.2. Targeted approach, outreach and oversight of at-risk non-profit organisations

383. There are 3 884 NPOs established in the Slovak Republic. In the NRA process, the NPOs operating in the territory were analysed, through the prism of potential misuse for TF purposes. The assessment is rather superficial and concluded that there are NPOs (including public collections), whose potential for misuse to support and finance terrorism is higher. In those cases, the funds raised were used to cover the costs of practicing religious rites, promoting or providing the necessary humanitarian aid, including food product, medicines and equipment. No suspicion of terrorist financing was found.

384. Turning to the monitoring, after reviewing of the entire NPO sector, SIS focused its attention on approximatively 2% of them, where risks were assessed more in detailed, in accordance with the intelligence priorities. Based on operative findings, the SIS performs regular supervision on some 6 – 7 sensitive NPOs, which does not appear to be fully commensurate with the size of the sector in Slovakia. The SIS monitors entities suspected of possible connection to TF and/or international terrorist networks. The review is done more on case by case basis rather than in a structured RBA manner.

385. The second LEA mainly charged with anti-terrorism financing duties, the CTU - NAKA, estimates the number of vulnerable NPOs at about 40[46]. Those NPOs were subject to monitoring.

386. According to the authorities, measures have been taken to increase communication and coordination between LEA, SIS and other relevant CT partners on NPO supervision. However, seeing the difference in the number of NPOs considered for supervision (SIS and CTU-NAKA), the AT is of the opinion that coordination on the matter is an area for improvement.

387. The authorities maintained that since no case or suspicions of NPO misuse for TF purposes has been identified, the general analysis of TF risks in the NRA would suffice. Nevertheless, the AT maintains the view that Slovakia has not thoroughly and consistently identified the types of NPOs which are vulnerable to FT abuse. The financial and non-financial activities of the some NPO sector have been assessed vis-à-vis the TF risk, but there is no specific risk ranking attributed to certain categories of NPOs.

388. The Register Office is the authority responsible for issuing licences for NPOs. According to the legislation, the Director of the NPO, is obliged provide his/her criminal records certificate to prove integrity. On the basis of the provided data, the Registry Office performs checks via the "Oversi" portal by requesting an extract from the criminal record from the GPO. Moreover, every NPO should have its own banking account before the registration which results in verifications done by the banks within the CCD procedures.

389. The NPOs have an obligation to send annual reports, and to inform on any changes in their activity. The annual report must contain certain statutory requirements. The Register Office shall ensure that the non-profit organization observes the declared purpose and provides the community services for which it was established. If this has not been done, the Register Office may file a petition to revocation the license for the non-profit organization.

390. In practice annual activity reports contain quite broad range of the information, and the Register Office checks whether the reports were filed. In some cases, the Register Office checks the accuracy of the financial flows reported but this is not done systematically. In case of failure to provide the necessary information (which is largely limited to the non-submission of the annual reports), the Register Office can and does impose sanctions (up to EUR1 000). For the period 2016-2018 there were 402 fines in the total amount of EUR55 680 imposed.

391. FIU is authorized to monitor NPOs for the purpose of identification of the BO or for the purpose of checking the use of the property they manage. The FIU shall initiate BO controls in case of donations of more than EUR1 000. Over the period under review, the FIU has conducted 4 inspections on NPOs during which two violations of the AML/CFT Act were found. The FIU published on its website a rather general guidance for the NPO on TF risks of potential abuse, and mitigation measures to be taken, but its impact on the private sector was minimal.

392. NPO sector is not organised into any professional or sectoral association that may facilitate the outreach activities or other forms of cooperation. Nevertheless, the NPO sector itself is aware to a certain extent of the TF risks. Risk mitigation measures are applied but not as a result of training or outreach by the authorities, but more due to rules and controls put in place by the major donors.

[46] Number provided for 2015

4.3.3. Deprivation of TF assets and instrumentalities

393. There has been no freezing under UNSCRs 1267 and 1373, and no instances of *"false positives"* have been reported. The REs and competent authorities have at their disposal legal mechanisms and instruments for applying freezing measures as described under the TCA.

394. There were no criminal freezing or confiscation orders in relation to terrorists, terrorist organisations and terrorist financiers. The authorities are currently conducting financial investigations (including identification of assets) in the context of three ongoing TF investigations (see IO 9), which may lead to the issuance of freezing orders.

4.3.4. Consistency of measures with overall TF risk profile

395. The Slovak Republic set threat and vulnerability rating for TF risks on a low and medium-low level, respectively. However, Slovakia did not assess different types of legal entities separately regarding their expose to ML/TF risks, including NPOs.

396. Despite the above shortcomings, the AT considers that the lack of TF designation and the absence of funds frozen are in line with the TF risk profile of the country.

397. In 2017 the special subgroup for combating TF and PF was established within the frame of NES-LP. This sub-group is responsible for analyzing the TF and PF context in SR, such as risks and threats, for developing rules on exchange of information among the members of the group, and for identifying of shortcomings in the TF and PF combatting mechanisms. The sub-group had only one meeting in 2017.

Overall conclusions on IO.10

398. The Slovak Republic ensures the implementation of UNSCRs 1267 and 1373 (and the successors) based in EU and internal legislation. The Slovak Republic has not received requests, proposed or made any designations pursuant to UNSCRs 1267 and 1373. No freezing measures occurred in accordance with UNSCRs 1267 and 1373 and no TF funds have been restrained, which is consistent with the overall TF country risk profile. The most material REs are well aware of the TF TFS and have a good understanding of their freezing and reporting obligations. Slovakia has not formally identified the types of NPOs which are vulnerable to TF abuse, but SIS and CTU-NAKA monitors some specific NPOs considered potentially more at risk. There is no outreach provided to the sector by the relevant competent authorities, only Guidance published on the FIU website. The Register Office performs checks on the NPO reports and imposes sanctions for a range of failure to fulfill the necessary information.

399. **Slovakia is rated as having a Moderate level of effectiveness for IO.10.**

4.4 Immediate Outcome 11 (PF financial sanctions)

4.4.1 Implementation of targeted financial sanctions related to proliferation financing without delay

400. Slovakia uses a combination of supranational (at EU level) and national mechanisms to implement PF-related TFS. The UNSCRs are incorporated into the EU Law, and thus into the national legislation of EU Member States, through Decisions and Regulations adopted by the Council of the EU. At national level, the ISA applies as in the case of TF TFS.

401. The EU mechanisms do not suffer from technical problems in relation to the time of their transposition when it concerns Iran. Individuals and entities had already been listed by the EU

when their designation by the UN was made. There are additional mitigating measures applied by the EU requiring a prior authorisation of transactions with designated Iranian entities. This allows the authorities to determine if the transfer of funds for which the authorisation is requested would be permissible according to the EU Regulations.

402. As for the TFS against DPRK, in the past, some designations by the UN were shortly transposed into the EU framework but in some other cases, delays in implementation of the UNSCRs of DPRK can still occur.

403. Turning to the communication of designations to the RE, it shall be noted that the MFA publishes links to relevant UNSCR (1718/2006 and 1737/2006, 1835/2008 and 2231/2015) on their website. The MFA webpage does not contain all relevant updates to the lists but refers to the main page of the UNSC which subsequently redirects to consolidated version of sanctions lists. The lists are available and accurate, and the authorities presented the AT with samples of letters sent from the Brussel Office to several state authorities flagging the fact that changes occurred in the lists.

4.4.2. Identification of assets and funds held by designated persons/entities and prohibitions

404. Financial institutions are generally aware of the need to have protocols in place to freeze any assets without delay as part of the implementation of PF TFS. While no obliged entities reported having to freeze assets or funds held by persons or entities designated under PF sanctions programs, there is no reason to doubt that financial institutions can take such steps effectively, at least as regards specifically named jurisdictions and persons.

405. No assets of persons linked to relevant DPRK or Iran UNSCRs have been identified in the country and as a result no assets or funds associated with PF have been frozen. There have been no investigations and prosecutions related to PF, including on border control. In the period under review, no UTR has been filed in relation to proliferation or PF in 2013-2018.

406. MoE is the authority responsible for control of trading in dual-use goods and issues licenses on trade with strategic goods which are subject to special regime. According to the information provided to the AT, upon receipt of a request for a trade in strategic goods, the MoE must request an opinion of the state authorities involved in the control of exports, transport and mediation of dual-use items[47]. Both MFA and the SIS are able to block granting a license. One license was refused in relation to Iran in 2015 based on the PF international sanctions.

407. In the area of double use goods, SIS cooperates with responsible state administration bodies (FACO, MFA, MoE and others) in the identification and prevention of export of material of double use which is not officialy declared as such, (*i.e* it is exported without the export permit). In addition, SIS makes preventive and awareness-raising activities for businesses regarding the potential misuse of exported dual-use goods and to underline their obligations with regard to exports to third countries.

4.4.3. FIs and DNFBPs' understanding of and compliance with obligations

408. The website of the MFA contains the links to relevant UNSCR (1718/2006 and 1737/2006, 1835/2008 and 2231/2015) which is the main communication channel for PF TFS related issues.

409. The most material FIs in Slovakia, are well-aware of their obligations on PF-related TFS. As in the case of TF TFS, the banks, the insurance companies and the securities intermediaries use international commercial databases to screen their clients or rely on self-developed software

[47] MFA, Ministry of Defense, MoI, Ministry of Health, FACO, SIS, Nuclear Regulatory Authority.

which include PF UNCSRs lists. Checks related to PF are done during the establishment of business relation with the client and in the context of the regular monitoring.

410. Exchange offices, non-bank payment institutions and most of the DNFBPs are moderately aware of TFS related obligations. They rely on manual, suspicion-based checks performed against the lists published through the MFA's website. Most of them mentioned that in case of PF TFS indications, they would consult the FIU before proceeding with the transaction. Lawyers and dealers of precious metals and stones have a very limited understanding of TFS related obligations and do not perform any PF related verifications of their customers. It appears that little is done to detect funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities.

4.4.4. Competent authorities ensuring and monitoring compliance

411. The NBS is the authority responsible for conducting monitoring for the implementation of UN TFS by the FIs. Supervision on implementation of TFS forms a part of inspections conducted in relation to banks by the NBS, although there is no supervisory risk model that would include issues on the implementation of UN TFS related to PFT. The later does not impact effectiveness since the PF TFS is not a risk-based obligation according to the FATF methodology.

412. The FIs confirmed that during the onsite inspections the implementation of UN TFS is considered by the NBS. In the course of on-site and off-site supervision in banks, the NBS verifies the inclusion of the PF international sanctions in the internal procedures and internal regulations and looks at the application of PF checks on a sample of clients and transactions. However, the general lack of resources dedicated to the supervision of the REs and the limited number and scope of supervisory actions undertaken by the NBS impact the effective monitoring of PF-related TFS (see IO 3). Turning to the rest of the financial sector, the NBS only screens the internal procedures of the REs to ascertain that the PF obligations are there. No sanctions for TFS breaches were imposed so far.

413. The FIU has no direct role or responsibility for the implementation and application of TSF pursuant to the ISA, as its supervisory functions derive solely from the AML/CFT Act. Hence, there is no authorized body to conduct monitoring for the implementation of UN TFS by the DNFBPs. In relation to TSF, the FIU only controls the CDD obligation under to ascertain whether the client or BO is a sanctioned person. When conducting on-site supervision, the FIU checks if the RE reported as suspicious *"transactions for which it is reasonably assumed that the customer or BO is a person covered by an international sanction or transaction for which it is reasonably assumed that its subject is or is to be a thing or service that can be related to a thing or service covered by an international sanction"*.

414. The Gambling Regulatory Authority established in June 2019 did not perform any supervisory activity for monitoring compliance with the UN TFS.

Overall conclusions on IO.11

415. Slovakia uses a combination of EU and national mechanisms for PF-related TFS which are implemented without delay when concerning Iran. Delays in the implementation of the UNSCRs of DPRK can still occur. No funds or other assets held by persons or entities designated under PF sanctions programs have been restrained so far which is in line with the country risk profile. The financial institutions understand their obligations and can take restrictive measures effectively should the situation occur. DNFBPs understanding and compliance with the PF related obligations are areas for improvement.

416. **Slovakia is rated as having a Moderate level of effectiveness for IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

5.1 Key Findings and Recommended Actions

Key Findings

1. Banks have a good understanding of ML risks and are aware of their AML/CFT obligations. Non-bank FIs have a satisfactory understanding and awareness of ML risks, with some weaknesses being identified in relation to MVT providers and exchange offices. The understanding and identification of sector/business specific ML/TF risks is not a general practice amongst the private sector. Turning to the DNFBPs, stronger knowledge was demonstrated by the auditors and (to a lesser extent) by casinos and notaries, while the dealers in precious metals and stones, real estate agents, tax advisors, accountants and lawyers have a moderate understanding of their compliance requirements. The lawyers, accountants and real estate agents lack full appreciation of their exposure to ML risks.

2. Understanding of FT risks by most FIs and DNFBPs is confined to screening sanction lists, which include UN designation lists and lists of jurisdictions.

3. Banks and most non-bank FIs demonstrated adequate application of basic customer due diligence (CDD) and record-keeping requirements with some shortcomings in the understanding of the concept of BO. All DNFBPs have basic understanding of CDD measures.

4. PEPs, their family members and close associates are treated as high-risk customers, although the application of specific measures varies across the sectors. FIs and DNFBPs mainly use a self-declaration for establishing source of funds and source of wealth without further verification. Only in a limited number of cases, which include mainly banks, information contained in the declarations is verified against data available in public declaration database of state officials.

5. Most of the FIs use sophisticated software tools to analyse risks and detect ML/FT indicators. While the procedures for reporting to the FIU are generally understood, the AT expected to see more UTR output from securities, exchange offices, MVTS, notaries, DMPS and lawyers.

6. There are several TF related UTRs sent to the FIU by both the financial and non-financial sectors. This is a positive outcome, but the AT is of the opinion that the set of TF suspicion indicators is limited, especially in relation to the geographical element which results in reporting based only on this factor.

7. Banks and larger non-bank FIs have put in place strong internal controls, which include various lines of defence: internal audit, automatic systems for transaction monitoring, periodic reporting to the management, access to commercial databases and appropriate human resources. Casinos and auditors appeared to have adequate internal policies and internal control procedures. Other DNFBPs (such as notaries, lawyers, real estate agents) do not have AML/CFT compliance structures in place as the majority of them are sole practitioners.

Recommended Actions

1. Authorities should ensure that exchange office, MVTS providers, and DNFBPs conduct regular assessments of their business specific ML/TF risks for customers, products and services. The risk assessments should be appropriate to the nature and size of the business and should consider the country risks.

2. Obliged entities should develop internal high-risk criteria specific to their sector and institution and apply EDD accordingly.

3. Non-bank FIs and DNFBPs should develop and implement mechanisms for a more systematic monitoring of transactions with a view to identifying ML/FT suspicions.

4. The authorities should require banks to apply necessary AML/CFT techniques for mitigation of ML/TF risks where non-face to face business is provided.

5. Supervisors should up-date or complement the sector-specific guidance, and broaden their training programs, to enhance ML/TF risk awareness and understanding of the preventive measures among the RE. Special attention should be given to the identification and verification of BOs, PEPs and to the TF indicators.

6. The FIU should provide UTR specific feedback to improve the reporting practice by the obliged entities.

7. Technical deficiencies (listed in the TC annex) relating to preventive measures should be addressed.

417. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The Recommendations relevant for the assessment of effectiveness under this section are R.9-23.

5.2. Immediate Outcome 4 (Preventive Measures)

418. Financial services are mainly provided by the banking sector, composed of 27 banks. Compared with the banks' market share in the economy, other financial institutions, including the insurance, securities, leasing companies, etc. account for only a marginal market share. Financial services are principally provided to residents of the country. Only 1 % of the total number of bank customers were non-residents, mainly natural persons from neighboring countries (Hungary, Ukraine, Czech Republic) and a few foreign legal persons doing business in Slovakia.

419. Banks pay significant attention to the ML/TF risks posed by non-residents and refuse to enter business relationships when there is no economic link with Slovakia. As per high risk customers (PEPs, persons residing in high risk countries, customers qualified as high risk on the basis of internal risk management systems), the share was around 3 % of the total number of customers.

420. All types of DNFBPs are present in the Slovak Republic except trust service providers. DNFBPs` sector has no specific features and the services provided by them are of a traditional nature.

421. Assessors' findings on IO.4 are based on interviews with a range of private sector representatives, as well as the experience of supervisors and other competent authorities concerning the relative materiality and risks of each sector. The AT grouped the obliged sectors into categories in terms of their significance in the overall picture of compliance (see Chapter 1).

5.2.1. Understanding of ML/TF risks and AML/CFT obligations

422. The understanding and identification of sector/business specific ML/TF risks is not a general practice among the representatives of the private sector.

423. Banks demonstrated a good level of understanding of sector specific ML/TF risks and respective AML/CFT obligations. All banks carry out enterprise-wide risk assessments periodically

and on an ad hoc basis (*e.g.* significant changes in business, new products, etc.). They identify different types of risks, such as client-related risk (*e.g.* PEPs, non-residents), country related risk (*e.g.* high risk, offshore countries), product-related risk (deposit accounts, loans, private banking), as well as transaction related risks based on typologies (*i.e.* tax evasion, fraud phishing schemes). Risks are classified into *"low"*, *"medium"* and *"high"* categories, and specific mitigation measures are taken accordingly. In the vast majority of cases, the risk assessments conducted by banks, especially where the bank is part of a group, are very comprehensive and include both institution specific and group specific risks. All banks were fluent in articulating the types and proportions of their institution-specific ML risks.

424. Some of the banks, especially larger ones, had a good level of understanding on risks connected with *"straw men"* used in company structures, as well as companies using *"virtual addresses"*. They also take appropriate mitigating measures, including enhanced due diligence measures, such as requiring additional documentation, checking real place of business, interviewing the customer. In some cases, these measures resulted in filing an UTR to the FIU or terminating the business relationship. The use of cash was considered as high risk by all the banks. In such cases special attention is paid to the source of the funds and wealth, purpose of the transaction, etc.

425. Understanding of AML/CFT obligations by almost all non-bank FIs is generally good. Life insurance, investment and leasing companies have clearer understanding of ML risks as opposed to payment institutions providing wire transfer services and exchange offices. The latter were unable to clearly articulate how ML might occur within their institution or sector, as well as demonstrated a lack of systematic understanding of AML/CFT obligations. Life insurance, investment and leasing companies conduct enterprise-wide risk assessments, and recognize the ML risks related to geographical location of the customer, PEPs, funds inconsistent with the source of wealth of the customer, extraordinary withdrawals or changes in the polices, etc. Non-acceptance of cash was stated by the representatives of the sectors as a mitigating factor.

426. Understanding of FT risks by most FIs is confined to screening sanctions lists, which include UN designation lists and jurisdictions. They did not demonstrate sufficient understanding of FT threats and vulnerabilities. Only one bank mentioned that specific TF related indicators were integrated into their IT systems (for e.g. an 18-year-old, non-resident person buying a ticket to a high-risk jurisdiction form his online account at midnight).

427. All banks, insurance, investment and leasing companies have proper understanding of their obligations related to TF risk mitigation in relation to UNSCRs and perform screening on customers with a view to freeze of assets of terrorists and terrorism related persons. The payment institutions providing wire transfer services and exchange offices lack understanding of TF risks and related CFT obligations.

428. The understanding of sector specific ML/TF risks is less developed among DNFBPs (with some exceptions) compared to the FIs. Auditors, casinos, notaries, and dealers of precious metals and stones, in most of the cases had more developed ML risk understanding compared to other types of DNFBPs. For example, casinos consider the highest risk being posed by online gambling, customers requesting a win certificate. The auditors consider higher risk customers legal entities with complex structures, or customers connected with tax havens. The notaries identified as higher risk those customers conducting high value transactions, while for the dealers of precious metals and stones- customers trading with precious metals and stones for investment purposes are more carefully handheld. Real estate agents stated that the risk of ML/TF is mitigated within their sector by the fact that in the majority of cases the property is purchased via bank loans and the necessary

measures are undertaken by banks. Lawyers and accountants did not acknowledge the existence of ML risks within their sectors (e.g. representing legal entities with complex structures, risks in relation to providing company services, unknown source of funds involved in the transaction), stating that criminals would not approach them in practice. The AT has no information suggesting that lawyers and accountant face often high-risk scenarios.

429. Among DNFBPs, relevant knowledge of the AML/CTF obligations was demonstrated by auditors and (to a lesser extent) by casinos and notaries. Certain DNFBPs, such as dealers in precious metals and stones, real estate agents, tax advisors and accountants, lawyers have a limited understanding of their AML/CFT obligations which are mingled with the business-related duties.

430. Understanding of FT risk and obligations is also limited to screening of terrorist lists, which include UN designation lists, and list of jurisdictions. However, they did not demonstrate sufficient understanding of FT threats and vulnerabilities. Some DNFBPs (particularly dealers of precious stones and metals) had no understanding of TF risk and respective obligations.

431. The vast majority of FIs with the exception of payment institutions providing wire transfer services and exchange offices, were involved in the NRA process through submission of questionnaires to the authorities and participation in the presentations of the results of the NRA. However, only banks rely on the findings of the NRA. Except for casinos, other DNFBPs neither participated, nor were aware or use the NRA.

5.2.2 Application of risk mitigating measures

432. The controls and mitigation factors which apply to the risks identified for FIs and DNFBPs under the AML/CFT Act are broadly applied. Customers are generally categorized as low, medium or high risk. Depending on the level of risk, simplified, standard or enhanced due diligence measures are applied.

433. All banks have sophisticated software tools to analyze risks and detect ML/FT suspicion indicators. The software allows for online checks against various open sources and databases and feeds the findings into the risk management system (i.e. identification of PEPs, sanctions and embargo list, high-risk countries, etc.). Banks classify their customers as high, medium or low risk. The main criteria for high-risk customers generally include those envisaged by AML/CFT Act, particularly domestic and foreign PEPs, non-resident customers, customers from high risk countries, countries with strategic deficiencies, customers using private banking services, cash intensive businesses or natural persons, legal persons with complex ownership structures etc.

434. Most FIs were aware of the additional measures required when a customer poses higher risk, including obtaining and analyzing supplementary documents on the nature of the business, source of funds invested and origin of the wealth, more frequent scrutinizing of transactions.

435. Despite having some level of ML/TF risk understanding, the DNFBPs demonstrated insufficient knowledge of the key constituents of an ML/ TF risk mitigation framework. There is an over reliance on the information provided by the customers (e.g. in case source of funds and wealth, PEP status) and further verification is not conducted properly by some non-bank FIs (exchange offices and payment institutions providing wire transfer services) and DNFBPs. Simplified due diligence measures are applied strictly in case of low risks identified only by some non-bank financial institutions and casinos. The other RE did not apply simplified due diligence measures.

436. The on-going monitoring regime is employed based on the customer's risk profile. In most of the cases, the banks and larger non-bank FIs perform automatic screening of their existing customers (on daily basis) to adjust their categorization and identify potential clients who have been listed (on the UN sanctions lists for instance), or who became a PEP after the inception of the business relationship. Controls are reviewed periodically, at least once a year.

437. The REs described under which circumstances they would decline to act for a customer or otherwise cease providing services. Almost all the representatives from the private sector mentioned that they refuse to conduct transactions or to establish business relationships when requested additional documents on the legal purpose of transactions, CDD or BO information are not presented. However, there were virtually no such denials or terminations of business among the non-bank FIs and DNFBPs, except for casinos, on AML/CFT grounds.

438. Risk-based decisions are taken by a number of FIs to restrict or exclude some business lines according to the risk appetite set in the AML/CFT internal rules. For example, none of the banks provides wire transfer services to walk-in customers.

5.2.3. Application of CDD and record-keeping requirements

FIs

439. FIs properly identify and verify customers and their representatives by obtaining the necessary identification data and verification documents. In the majority of cases, initiation of the business relationship is conducted with the physical presence of the customer. For identification purposes customers are required to present their IDs, fill in the questionnaires describing the nature of their business, source of funds and wealth (in case of ML/TF high risks), and provide relevant KYC documents, contracts, information related to the management and ownership structure of the company. The identification and verification procedures for customers that are natural persons are applied to directors and other legal representative of legal persons and BOs. If the provided data is incomplete, the FIs refuse to cooperate with the client. In the verification process, FIs mostly use several public databases (Stolen ID cards, Register of public sector, Commercial register, etc.), as well as their own analytical tools. Banks and larger non-bank FIs also use international paid databases (Down Jones, World Check, etc.).

440. To understand the purpose and intended nature of business relations, FIs obtain the information from customers on the types of services sought, expected transaction volumes and check their main activities. For corporate customers their main business partners are checked via public sources. In some cases, visits are made to the customers premises (for mitigation of risks with regard to virtual seats of legal persons). This information is used to establish a profile of the customer which will be used during the monitoring of their on-going activities.

441. FIs met on-site stated that they do always identify natural persons behind the customer. However, the on-site interviews revealed certain gaps in the understanding of the concept of beneficial ownership. In particular, the difference between beneficial ownership and ownership interest is not fully appreciated, thus, natural persons holding relevant management positions or exercising indirect control over the customer are not always sought after. As a result, majority of the FIs determine the BOs primarily based on legal ownership and heavily rely on self-declarations. Banks and FIs that are part of larger groups also check foreign databases and receive support from parent groups. Additional verification of BO is conducted if higher risk criteria are identified (e.g. complex legal structure involving two or more legal persons in the ownership chain, foreign ownership). The authorities stated that they mainly rely on banks with regard to BO identification and are satisfied with the quality of information held by banks.

442. There are exemptions from CDD requirements provided by the AML/CFT Act (see IO1 and R1), but these exemptions are not applied by the FIs in practice.

443. Non face-to-face business relationships, as well as third party reliance are not a common practice in Slovakia. Non face-to-face services are mainly provided by banks (including when establishing business relationship) and are considered as high-risk scenarios requiring enhanced due diligence measures. These include identification and verification through video call, and more frequent ongoing monitoring. Additional verification measures are taken, e.g. sending a letter to the customer's registered address, to ensure that the addressee is aware that a bank account is being opened on his/her behalf. However, it appears that the enhanced due diligence measures applied to the non face-to-face business relationships, are more focused on fraud prevention than AML. Not all AML/CFT techniques are used to mitigate the ML/TF risks (*e.g.* not all banks require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards).

444. Ongoing monitoring mechanisms vary across the FIs. Most of the FIs described transaction monitoring, customer screening and CDD updates as part of ongoing due diligence applied. Banks and larger non-bank FIs (insurance, investment and leasing companies) use sophisticated IT systems that employ built-in scenarios to identify unusual activities or connections, while smaller non-bank FIs examine transactions manually. Checks are generally tailored to the risk level. FIs update CDD data regularly and high-risk customers are subject to more frequent updates. Such updates include examining whether transactions carried out are consistent with customer profiles or expectations about the intended nature of business relations.

445. Deficiencies with regard to CDD, including ongoing monitoring exist in non-bank payment institutions providing wire transfer services and exchange offices. Payment institutions providing wire transfer services identify and verify customers when carrying out single transactions exceeding EUR1 000 or when concluding business relationships. They have a moderate understanding of some constituents of CDD processes. Although aware of basic CDD requirements, the exchange offices mainly rely on the information provided by the customer and do not conduct further verifications and analysis.

446. All FIs are well aware of their record-keeping obligations. Often stricter rules compared to the FATF requirements are in place for the maintenance of customer identification data, account files and business correspondence. The supervisory authorities have not identified any serious deficiencies in this respect.

DNFBPs

447. Application of CDD and record-keeping measures varies among DNFBPs, but is generally much less comprehensive compared to the financial sector.

448. Notaries generally observe the CDD requirements, mostly due to their professional profile and type of services provided. Notaries obtain basic identification data of customers and inquire if they act on somebody else's behalf. However, some of the BO requirements, such as checking the source of funds, are insufficiently applied. Notaries are unfamiliar with the requirement of conducting ongoing due diligence of their customers.

449. Auditors strictly follow the international auditing standards, which also include AML procedures, identify customers and verify the authority of their representatives. Auditors also request customers to fill questionnaires stating their UBOs and describing their business activities as part of their reputational risk management, although further verification of the information, except for checking it against state registers, is not carried out.

450. Casinos perform CDD on their clients at the entry to the premises. Identification is done through an official document, which is scanned and verified against state databases (e.g. Stolen ID card database). If a customer refuses to be identified, he/she is denied the access to the premises. CDD includes source of funds declaration, however, since no verification is done, no refusals are made based on inconsistent information on the source of funds. This exercise appears to be rather formalistic and does not enable the detection of possible ML activity.

451. Real estate agents conduct CDD of both purchasers and vendors of the real estate property which includes only identification and verification of the customer. Real estate agents do not have sufficient understanding of the UBO concept, and therefore do not find it necessary to identify the UBO of the client.

452. Dealers of precious stones and metals are de facto excluded from CDD obligations, since they are not allowed to conduct cash transactions above EUR15 000. Other DNFBPs, including accountants, tax advisors and lawyers have very basic perception regarding the CDD process.

453. All DNFBPs stated that they would refuse to enter into a business relationship or to conduct a transaction in case of incomplete CDD. Record keeping requirements are generally observed among all DNFBPs, except for real estate agents. Real estate agents keep only accounting documents related to the transaction, which is insufficient to comply with the FATF standard. As indicated by the authorities, the few real estate agents which have been subject to inspections were able to provide all CDD related data.

5.2.4. Application of EDD measures

PEPs

454. The legal framework covers both foreign and domestic PEPs. All FIs and DNFBPs were aware of the PEP definition and related CDD measures. While FIs, except for exchange offices and non-bank payment institutions, use automated systems and databases to ascertain the PEP status of existing or potential foreign customers, DNFBPs, except for casinos, referred to self-declarations made by the foreign customers on their status. For local customers, the FIs and DNFBPs referred to asset declarations made at national level, or their internally developed lists. Ascertaining a local PEP is not difficult in Slovakia due to the small size and population of the country. All FIs and DNFBPs interviewed, including banks, found it challenging to define close associates of PEPs and admitted experiencing practical difficulties in identifying those.

455. Where PEPs, family members and close associates are identified, FIs and DNFBPs treat them as high-risk customers, although the application of specific measures varies across the sectors. FIs referred to senior management approval, establishment of the sources of wealth and funds and enhanced on-going monitoring as a part of the usual business practice in relationships with PEPs, their family members and close associates. DNFBPs were generally aware of the need to apply EDD in case of PEPs. Nevertheless, the examples provided on the actions taken in practice did not cover all the requirements, therefore, the AT concluded that there is limited understanding on what enhanced measures would entail after a PEP is identified. FIs and DNFBPs mainly use a self-declaration for establishing source of funds and source of wealth without further verification. Only in a limited number of cases information contained in the declarations is verified against data available in public declaration database of state officials.

Correspondent Banking

456. There are a few banks providing correspondent banking services to respondent institutions which are generally EU banks belonging to their group. In these cases, EDD is carried

out. When conducting EDD the following measures are applied - submission of questionnaires with specific questions on control mechanisms, business nature, and requiring senior management approval before the relationship is established. Banks also make sure that correspondent relationships do not involve shell banks, while payable-through LORO accounts are not allowed. Correspondent relationships are subject to periodic reviews.

New Technologies

457. All FIs interviewed were aware of the requirement to assess the ML/FT risks related to the implementation of new services and products, and the use of new (developing) technologies in business. The involvement of the compliance officer, who is responsible for ML/TF risk assessment and mitigation, is mandatory in this process. DNFBPs did not report any current or planned operations assuming use of new products, practices (including delivery mechanisms) and technologies.

Targeted Financial Sanctions

458. The level of awareness regarding implementation of TFS varies across different sectors. All banks and several other FIs demonstrated satisfactory awareness of their TFS obligations. Some sectors, such as exchange offices, payment institutions providing wire transfer services, lawyers and dealers of precious metals and stones have a more limited understanding of TFS related obligations.

459. Most FIs implement automated IT solutions for screening customers (including UBOs) against UN and EU lists, with the exception of some participants of the securities markets and exchange offices. The IT solutions also include automated screening of all customer base against the updates made in the lists. DNFBPs do not conduct regular screening against lists, with some notaries, real estate agents and casinos checking lists through the website of the MFA when they have foreign clients. There are some concerns over the depth and timeliness of their checks.

460. Lawyers and accountants do not have any understanding on TFS and confused them with higher risk countries and related obligations.

461. Most FIs and DNFBPs were relying on commercial databases and were unaware of any lists and guidance being provided by the authorities.

462. FIs were aware of their freezing and reporting obligation. Some banks mentioned that simultaneously to reporting on freezing to the FIU they will inform the NBS and the MoF.

463. Transaction monitoring to detect possible sanctions evasion was performed by some of the banks. Other FIs and DNFBPs demonstrated limited awareness on the importance of transaction monitoring.

Wire transfer rules

464. MVTS are provided through banks and payment institutions providing wire transfer services who act as agents of global MVTS providers (MoneyGram, Western Union etc.). Banks provide MVTS only for their customers, the wire transfer information being automatically screened by the system. Checks are carried out periodically to ensure that wire transfers contain all required data. In cases of missing information, banks contact the originator's institution and request additional information, before proceeding with the transfer.

465. Payment institutions who act as agents of global MVTS providers and provide occasional wire transfer services have very limited understanding of their obligations with regard to R 16, including screening and rejecting non-complete transaction. Considering the lack of supervision of

the agents of the MVTS providers and the lack of information on the modalities applied by the authorities for identifying the provision of unauthorized payment services by persons other than authorized institutions (please see IO3 for further details), no conclusions can be reached as to the level or adequacy of compliance with these obligations.

Approach towards jurisdictions identified as higher-risk

466. All FIs and most DNFBPs demonstrated satisfactory awareness of their obligation to assess geographical risk factors when identifying whether there is higher risk of ML/FT. The following are considered to pose a higher risk: countries identified by the FATF as having strategic deficiencies; countries identified as having a significant level of corruption or other criminal activity and countries subject to sanctions, embargos or similar measures issued by, for example, the EU or the UN. Banks and larger non-bank FIs consider also all non-EU countries, offshore countries, as well as countries identified as posing higher risk at a group level.

467. In case of links with high-risk jurisdictions, the EDD measures are aimed at determining the purpose and nature of transfers, the source of funds involved in the transfers, relationship of the customer to the respective country etc. Dealers of precious metals and stones and accountants had poor understanding of higher risk countries and did not refer to the application of any EDD measures.

468. Representatives of the private sector are rarely provided with lists or guidance on high risk countries by the FIU and supervisory authorities.

5.2.5. Reporting obligations and tipping off

469. All FIs and DNFBPs are aware of their suspicion reporting obligations. Some non-bank FIs and DNFBPs have not filed any UTRs nor identified any cases when suspicions have been discussed internally. Most non-bank FIs and DNFBPs were unable to elaborate on typologies, transactions or activities that would give rise to a UTR, particularly in relation to FT. For the majority of DNFBPs the absence of UTRs was justified by the limited vulnerability to ML /TF activities.

470. Although it is very common to refuse the establishment of a business relationship or not to conduct a transaction in case of suspicion, only the banks would consider submitting UTRs to the FIU in this case.

471. Banks and larger FIs also maintain a *"black list"* of customers (e.g. behavioral patterns or none cooperative nature of some customers are amongst the reasons for a customer to appear on the list, group wide provided lists, etc.). Most UTRs are filed for suspicions related to tax evasion, unknown origin of funds and *"virtual addresses"* of legal persons. Banks, as opposed to other FIs and DNFBPs, also consider and file UTRs with regard to TF suspicions.

472. The statistics on reporting are provided and elaborated on under IO 6. It is evident, that substantial majority of UTRs are submitted by banks, which is consistent with the materiality of the sector. However, the AT considers that the reporting patterns by some FIs and DNFBPs (namely exchange offices, MVTS, notaries, lawyers, dealers of precious stones and metals) is not fully justified by the ML/TF risks in the sectors. A reason appears to be the low level of understanding of specific ML/TF risks.

473. With regard to the DNFBP sector, casinos demonstrated higher awareness of suspicious transaction indicators and frequently submitted UTRs, mostly related to cases of criminal background of the client, unknown source of funds or card fraud. The low level of reporting by some DNFBPs, in particular lawyers, notaries and auditors, appears to be inconsistent with the risks identified in these sectors.

474. FIs and DNBPFs submitting UTRs are generally satisfied with the feedback provided by the FIU. Nonetheless, several suggested that feedback is mostly very general consisting of the overall number of UTRs and disseminations. Although this was not consistent across entities interviewed, the AT considers that feedback on entity-specific UTRs, with indications of additional information on reasoning would be more appropriate.

475. FIs and almost all DNFBPs (except for real estate agents) demonstrated proper understanding on importance of tipping-off obligations. However, the legislation does not permit REs to refrain from CDD when this might alert the customer. Practical measures to prevent tipping-off include limiting communication between the front offices (who could tip-off the client) and the Compliance (in charge of the UTR filing) regarding the submission of an UTR. Training conducted internally by FIs and most DNFBPs include matters related to tipping-off.

5.2.6. Internal controls and legal/regulatory requirements impending implementation

476. Most of the private sector entities have compliance officers with sufficient seniority, independence and knowledge of the institution's ML/FT risk exposure. They are responsible for taking decisions affecting the institution's risk exposure.

477. Internal controls to ensure compliance with the AML/CTF requirements were described by banks and larger non-bank FIs to include an independent compliance and audit function. The compliance officer has unrestricted access to the whole subset of information within the entity.

478. Banks and non-bank FIs, which are members to financial groups implement group-wide policies and procedures for the prevention of ML/FT, which in practice have more strict regulations than the national legislation. At least one member of the board is responsible for the implementation of AML/CFT measures. All banks and larger FIs have appropriate control systems in place to mitigate ML/FT risks. Those controls are based on a 3 lines of defense model and include: 1st line - the customer facing staff, who reports the suspicions and high risk indicators to the AML/CFT compliance staff, 2nd line - the AML/CFT compliance staff, who is responsible for monitoring, analyzing and reporting the transactions, assessing ML/TF risks of the institution, etc., and the 3rd line - the internal audit, performing risk based audits of the 1st and 2nd lines. Internal controls also include automatic systems for transaction monitoring, periodic reporting to the management, access to commercial databases and appropriate human resources. They seemed to be sufficiently staffed. Periodic AML/CFT trainings are organized for staff. Specific training is organized for new staff and for management.

479. Casinos and auditors appeared to have adequate internal policies and internal control procedures. Casinos reported that training is provided for staff periodically. Other DNFBPs (such as notaries, lawyers, real estate agents) do not have AML/CFT compliance structures in place as the majority of them are sole practitioners. However, all of them had AML/CFT programs in compliance with the requirements of the AML/CFT Act.

480. There are no legal or regulatory requirements, which impede the implementation of internal controls and procedures to ensure compliance with AML/CFT requirements. Most of the banks and non-bank FIs are members to financial groups and there are no difficulties in the transfer of customer or CDD information within these groups.

481. No major issues on the internal controls of RE have been identified by the supervisors through inspections.

Overall conclusions on IO.4

482. The banking sector demonstrated a proactive approach to risks and good understanding of their AML/CFT obligations. The understanding of sector specific ML risks is less developed among DNFBPs (with some exceptions). Most FIs demonstrated adequate application of preventive measures with most common shortcomings being in relation to the understanding of the concept of BO. All DNFBPs have basic understanding of preventive CDD measures. Banks and larger non-bank FIs have put in place strong internal controls, which include various lines of defense. Casinos and auditors appeared to have adequate internal policies and internal control procedures.

483. **Slovakia has achieved a Moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

6.1. Key Findings and Recommended Actions

Key Findings

1. The FIU and sectoral supervisors (the NBS and the Gambling Regulatory Authority) share responsibility for supervising FIs and DNFBPs with the AML/CFT legislation. The NBS and the Gambling Regulatory Authority exercise their mandate for controlling compliance with all applicable AML/CFT requirements of FIs and casinos except the one on reporting to the FIU, respectively. In case the NBS identifies a failure to submit UTRs, this information is provided to the FIU. The FIU also inspects the compliance with the AML/CFT requirements, including with the reporting obligations. While there is some cooperation between the FIU and the NBS, mainly regarding issues related to ST reporting, the cooperation between these two authorities needs to be further improved.

2. The ML/FT risk understanding among the supervisory authorities varies and is mainly based on the results of the NRA. The FIU and the NBS demonstrated a satisfactory level of understanding of the general ML/FT risks in their supervised sectors. The Gambling Supervisory Authority demonstrated a low level of understanding of ML/FT risks.

3. The scope and the depth of the inspections conducted by the FIU and the NBS are not fully based on the AML/CFT risks. The reason behind is the lack of a documented process in place, which sets out how subject person specific ML/FT risk-ratings drive the frequency, the scope and the nature of future supervisory onsite/offsite inspections, as well as the lack of resources available for AML/CFT supervision.

4. At the time of the onsite visit there was a lack of offsite or onsite inspections of the MVTS sector. Considering the level of understanding of their obligations among the MVTS agents, this is an area for concern.

5. AML/CFT issues in the gambling sector have been covered to some extent during the holistic supervision conducted by the former supervisor (Ministry of Finance). As for the newly established (2019) Gambling Supervisory Authority, at the time of the on-site visit, no AML/CFT inspections have been carried out.

6. The NBS has in place established fitness and properness checks to prevent criminals and their associates from owning or controlling FIs, which seem adequate. However, it is not clear that the measures for monitoring on-going compliance with fit and proper requirements are always effective.

7. The entry to the Casino sector is subject to a set of controls which include verification of criminal records on management and owners. Lawyers, notaries, tax advisors, accountants and auditors are subject to professional standards and criminal record checks. No checks are being conducted to prevent the criminals' associates from entering these sectors and professions.

8. Although a wide range of sanctions is available for the authorities (both for natural persons and legal entities), the level of sanctions applied so far cannot be considered dissuasive. Moreover, no sanctions have been applied to the management of RE.

9. In the view of the limited number of inspection and the level of sanction applied, it is questionable that the supervisory actions undertaken have an impact on compliance with

AML/CFT obligations by the obliged entities.

Recommended Actions

1. The supervisors should continue to enhance their knowledge on the reporting entity sector specific ML/FT risks. They should review their risk-based approach and introduce comprehensive risk based supervisory model, which would be risk-ratings driven in terms of frequency, scope and nature of supervision.

2. The newly established Gambling Authority should develop an AML/CFT risk-oriented supervision.

3. The supervisory authorities should allocate more resources and expertise to undertake full risk-based supervision of FIs and DNFBPs. The NBS should consider devoting staff only for AML supervision onsite and offsite.

4. The level of cooperation between the supervisors should be enhanced both at the licensing stage and when conducting supervisory activities.

5. The Slovak Republic should ensure that regular review is conducted to ensure ongoing compliance with fit and proper requirements. The authorities should ensure that associates of criminals are prevented from entering the following sectors and professions: casinos, lawyers, notaries, tax advisors, accountants and auditors.

6. The NBS should undertake measures for identifying breaches of licensing or registration requirements and should ensure that MVTS agents are subject to supervision.

7. All supervisors should reconsider the criteria for the application of sanctions to ensure that dissuasive sanctions are applied to address violations of AML/CFT obligations.

484. The relevant Immediate Outcome considered and assessed in this chapter is IO.3. The Recommendations relevant for the assessment of effectiveness under this section are R.14, R. 26-28, R.34, and R.35.

6.2. Immediate Outcome 3 (Supervision)

485. The FIU and sectoral supervisors (the NBS and the Gambling Regulatory Authority) are assigned shared responsibility for supervising AML/CFT compliance of FIs and DNFBPs. The NBS and the Gambling Regulatory Authority exercise their mandate for controlling compliance of supervised entities with all applicable AML/CFT requirements except the one on reporting to the FIU. The FIU exercises supervision of compliance of supervised entities with all applicable AML/CFT requirements, including reporting to the FIU.

486. Positive and negative aspects of supervision were considered in light of their significance as described under Chapter 1.

6.1.1 . Licensing, registration and controls preventing criminals and associates from entering the market

NBS – FIs

487. The *"fit and proper"* decisions are made through the EU Single Supervisory Mechanism (SSM) for members of the management board and supervisory board of the significant banks in the Slovak Republic, and for qualifying shareholders of all banks.48

488. In November 2014, the NBS became part of the SSM, which is the first pillar of the Banking Union. As part of the EU SSM, Slovakia counts nine significant banking entities (https://subjekty.nbs.sk/?aa=select_categ&bb=8&cc=&qq=) under the direct prudential supervision of the European Central Bank (ECB). Under the SSM, the ECB grants authorisations to banks based on their applications to the NBS. In relation to "fit and proper" requirements for the persons responsible for the management of banks and acquisitions and disposal of qualifying holdings in banks, the final decision is made through SSM.

489. The NBS remains directly responsible for approving members of the management board and supervisory board and acquisitions of the remaining banks and other FIs (total of 27 banks in RS of which 9 are under direct prudential supervision of the ECB and 18 supervised directly by the NBS).

490. The NBS applies fitness and properness measures to prevent criminals and their associates from holding or being the BO or holding a management function in the FIs.

491. The fit and proper tests are applied to the applicants and BOs, members of the statutory body, administrative board and supervisory board, as well as other senior executives of the financial institutions. This includes competency and integrity checks. Although the AML/CFT Act does not explicitly require that the "fit and proper" assessment applies also for the compliance officers designated pursuant to art 20(2) (h) of the AML/CFT Act, the authorities clarified that in practice *"fit and proper"* tests are applied for the compliance officers too.

492. This information is submitted by the potential applicants through declaration. By signing the declaration, the applicant certifies that all data and documents supplied, including certified copies of documents, are complete, correct, true, genuine and up-to-date. The authorities have advised that the NBS conducts a number of checks to verify the provided information, including requesting information on the criminal background from the GPO; making requests to foreign counterparts if the potential applicant has similar license form foreign jurisdiction; checking information on education and previous work experience. The applicants are also checked against the list of persons subject to TFS.

493. No specific examples of cooperation with foreign supervisors or other counterparts have been provided by the authorities.

494. During the licensing or market entry process in case of doubt about the trustworthiness of the information provided by the applicant or about the source of funds, the NBS requests the FIU information on the applicant, namely if the applicant has violated AML/CFT legislation or if the applicant has been subject to administrative or judicial proceedings.

495. Background checks are extended to associates, relatives or affiliates. This information is requested through declaration, which is being checked for accuracy. The NBS also requests information on possible links with PEPs and verifies the CVs of the applicants regarding past or present public functions. An exception was found in the insurance sector, where potential links with PEPs are not considered.

---

48 The ECB has the power to make fit and proper decision only for the banks which are considered as significant. National authorities are responsible for fit and proper decisions in relation to less significant banks.

496. During the licensing process, the BO related information is checked against national or foreign BO registers (if BO register is available in a foreign country). If a BO register does not exist in a foreign country, official documents for verification will be requested from the applicant. As for the national BO register, at the time of the on-site it was being populated with information.

497. Checks are carried out during onsite inspections to identify any changes occurred after authorization has been issued. However, the NBS does not regularly screen the persons holding a significant or controlling interest or management function in an FI, therefore, the system is reliant on the licensed community to self-report any changes.

498. There was a moderate number of new entrants into the finance sector in recent years (see Table 36 below). There were 4 cases of formal refusal of application for non-banking creditors at the pre-licensing stage. The reasons for the refusal of these applications were failure to prove clean and trustworthy origin of funds, or failure to prove the credible origin of the deposit used for the registered capital. The main reason for withdrawing an application, was requests for additional information from the NBS side, which made the subjects withdraw their request for license.

Table 36: Number of licence applications received by the NBS (2015-2019)

Licence Applications	2015	2016	2017	2018	2019
Received	78	74	58	40	52
Approved	64	75	54	35	50
Withdrawn	8	14	4	8	3
Refused	0	1	3	0	0

Table 37: Licence applications by the type of subject person

Licence Applications		2015	2016	2017	2018	2019
Received	**Banks**	1	0	0	0	0
	Payment Institution	2	2	1	2	1
	E-money institutions	1	0	0	0	0
	Currency exchange operators	11	15	13	17	17
	Non-banking creditors	0	9	3	4	1
	Securities companies	1	2	4	1	2
	Intermediaries	24	45	37	15	30
	Insurance companies	0	0	0	0	0
	Coll. Invest funds	4	1	0	1	1
Withdrawn and Refused		10%	23%	9%	20%	6%

499. Licenses are revoked if there are breaches of the license conditions identified in the course of supervision, or in case serious triggers (e.g. receiving adverse information from public sources) are confirmed.

500. The supervisors do not actively police the perimeters to detect any unlicensed service providers. The authorities stated that they would rely in practice on whistleblowers to identify unlicensed activity, and on complaints filed with Financial Consumer Protection Department of the

NBS by customers. This issue is of particular concern in the case MVTS agents, as no supervisory activities were being conducted with regard to the MVTS.

Casinos and Online Gaming

501. Casinos (including those operating via internet) are required to be licensed by the Gambling Regulatory Authority since June 2019. Before, the licenses were issued by the Ministry of Finance. Entry to the Casino sector is subject to a set of controls which include verification of criminal records on management and owners of casinos. In case of suspicions, further checks are conducted. However, these measures do not cover the associates of criminals and are only applied at the licensing stage. There are also no checks applied to identify UBOs of the applicant. The GRA verifies the documents submitted by the applicant and checks the compliance with the Law on Gambling.

502. There were no cases when the application for a license has been refused by the authorities or the applicant has withdrawn the application for a license.

503. As indicated by the GRA, a specialized unit is searching open sources to find information on any unlicensed activity, in some cases information being received from the whistleblowers to identify any unlicensed service providers.

Other DNFBPs

504. Lawyers, Notaries, tax advisors, accountants and auditors operate systems aimed principally at professional standards, with adequate criminal checks.

505. Notaries are subject to licensing. The license is granted by the MoJ, the selection process being conducted by the Chamber of Notaries, which supervises the notaries registered in the Central Notary Register.

506. Integrity and good reputation of notaries is checked before granting a license. A candidate must provide a list of documents including a criminal certificate on absence of criminal records.

507. There were no examples of withdrawal of licenses and it is not clear if any checks are being conducted after issuing the license.

508. Lawyers are also subject to licensing. In order to be a lawyer in Slovakia one has to pass an exam to enter the Slovak Bar Association. Integrity of lawyers is checked, and a criminal record is requested. There were no examples of withdrawals of licenses and it is not clear if any checks are being conducted after issuing the license.

509. Accountants, tax advisors and auditors, real estate agents and traders in precious metals are also required to present a criminal record and proof of integrity.

510. No checks are being conducted to prevent the criminals' associates from entering these professions.

1.1.2. Supervisors' understanding and identification of ML/TF risks

511. The FIU and the NBS demonstrated a satisfactory level of understanding of the general ML/FT risks in their supervised sectors. There are weaknesses in the appreciation of specific ML/FT risks by the GRA.

512. The ML/FT risk understanding of supervisory authorities is mainly based on the results of the NRA and to some extent results of supervisory activities, information exchanged with foreign

supervisory authorities, supra-national risk assessment conducted by the EU, and in case of the FIU the number and the content of the UTRs.

513. To improve it's understanding of risks and to identify new risks, the FIU uses information from the NBS, and the private sector. The AT considers that the information exchange between the NBS and the FIU is very limited due to the legal shortcomings and it relates to specific cases of breaches identified or sanctions applied with regard to financial institutions. This is not sufficient to improve the overall understanding of the FIU on the risk-level of different sectors and the risks at all subject persons.

514. The NBS informed its understanding of ML/FT risks through the review of internal AML/CFT rules, risk assessments and answers to the questionnaires circulated by the NBS on a regular basis. Based on those evaluations, the NBS identifies current ML/FT trends and risks and uses the results to target areas of focus in its supervisory actions. The NBS co-operates with the FIU and foreign supervisory authorities. The NBS also uses information obtained from on-site or off-site supervision. The method is not based on detailed information on products, customers or distribution channels, therefore the AT cannot conclude that the method used enables the NBS to broadly understand and especially identify risks.

515. The new GRA is strengthening its knowledge of ML/FT risks by preparing procedures/methodologies on risk-based approach. These documents were at the drafting stage at the time of the onsite. The AT considers that the gambling supervisory authority lacks full understanding of ML/TF risks.

1.1.3. Risk-based supervision of compliance with AML/CFT requirements

516. The NBS, the GRA and the FIU are assigned responsibility for supervising AML/CFT compliance of FIs and casinos. In practice the NBS and the GRA exercise their mandate for controlling compliance of supervised entities with all applicable AML/CFT requirements, except the one on reporting to the FIU. In case the NBS identifies failure to submit UTRs, this information is provided to the FIU. The FIU inspects the compliance with all AML/CFT requirements, including the reporting obligation and in case there is a need to apply sanctions, this will be done by the NBS. The FIU will be subsequently notified about the application of sanctions.

517. The FIU is the supervisory authority for all the DNFBPs other than casinos. There is cooperation between authorities to avoid overlap in supervisory and sanctioning activities, however there is lack of cooperation in exchanging information for assigning risk ratings to the financial institutions and making decisions on the supervisory plans.

518. The NBS has risk rated each sector under its supervision based on the results of the NRA, the numbers of UTRs, self-assessment questionnaire, results from the previous AML/CFT onsite inspections and ongoing off-site monitoring determining the importance of each sector. The banking sector (medium high) has the most complex rating but each sector is reassessed periodically (annually) or if there is a risk event that conducts to significant changes. .

519. For AML/CFT rating of individual FIs the NBS uses in its risk assessment system qualitative criteria like (i) organization of the AML system, (ii) staffing arrangement (ownership and company structure, reputation of management, value of assets), (iii) customer identification process, (iv) know your customer and customer's categorization (including politically exposed persons), (v) record keeping, (vi) AML/CFT internal rules for prevention, (vii) the process of suspicious transactions detection and reporting to FIU, (viii) mechanism of internal AML/CFT controls and

(ix) the AML/CFT trainings, (x) measures and procedures against terrorist financing. Previously identified shortcomings are also considered for the risk classification of FIs.

520. Although the NBS uses qualitative data to assess AML/CFT risks, there is no actual and documented risk level classification, a risk map or risk matrix for each financial institution. The risk-based approach of the NBS would benefit from a documented assessment of the whole population of supervised entities applying risk-based approach at the level of individual entities supervised and at the level of sectors. The evaluation team was not provided with a documented procedure setting out how these risk-ratings drive frequency, scope and nature of onsite and offsite inspections.

Table 38: Risk rating of the FIs by the NBS

Industry Sector	Total Population (end of 2018)	Population Not Risk Rated (%)	High Residual Risk Population	Medium Risk Population	Low Risk Population
Banks	26	0	5	9	12
Securities companies	20	0	0	4	16
Insurance companies	14	0	0	11	3
Asset management companies	8	0	0	8	0
Supplementary pension management companies	4	0	0	0	4
Pension fund management companies	6	0	0	0	6
Other FIs/*IFA independent financial agent, FA financial adviser,	IFA+ FA 531	0	14	0	517

521. The NBSs Banking and Payment Services Supervision Section; Insurance Supervision Section and Capital Market and Pension fund Off site Supervision Section are in charge for AML/CFT supervision of the FIs.

522. The NBS supervisory staff responsible for prudential and AML/CFT supervision consists of 14 members. The segregation of supervision departments enables the NBS to allocate resources to all entities. Onsite inspections include examining the implementation of TFS. As indicated under Table 39, the NBS has dedicated some resources to deal with a small number of thematic AML/CFT inspections. The lack of staff devoted for AML/CFT supervision impacts the intensity of the supervision.[49]

523. For the purposes of offsite supervision, a questionnaire containing the set of questions on the AML/CFT compliance framework is sent to all banks once a year. Similar questionnaires are sent to insurance companies every 1 to 4 years.

[49] As indicated by the authorities after the on-site visit there was a restructuring in the NBS and separate AML/CFT supervisory unit has been established. As this change occurred after the on-site visit the effectiveness of the work it has not been subject to analysis by the assessment team.

524. In the securities' sector, evaluation of information and background documents is carried out by a questionnaire. Offsite supervision for the securities'' sector is conducted every 2 to 4 years.

525. For other types of financial institutions providing financial intermediation and financial advisory services, the NBS has implemented a reporting information system "Regfap" through which the entities will electronically submit on a quarterly and annual basis information regarding, *i.a.* number of UTRs submitted to the FIU, number of cash transactions of more than EUR 10 000, number of transactions of more than EUR 10 000 and shortcomings identified by inspections. "The annual financial intermediation report" submitted through "Regfap" is mandatory for each financial sector entity but this systmen started operating only since 1 anuary 2019.

526. The NBS has informed the evaluation team about its own risk-based methodology (not enforceable) based on which on-site supervision is carried out.

527. AML/CFT on-site inspections, which are mostly part of the annual plan, form a part of comprehensive on-site supervision (timeframe from 2 to 4 weeks) with a team of 3 or more members depending on the size and complexity of the supervised entity. Coverage of onsite inspections include also AML/CFT elements, including internal AML/CFT program, employee training, CDD, UT reporting, internal inspection, implementation of TF related targeted financial sanctions, client and transaction sample review. The NBS is also conducting thematic AML/CFT inspections. The NBS decides on the length of investigation taking into consideration the information provided by the entity and the type of the entity.

528. During the on-site inspection the supervisors focus on the following areas: the concept and basic principles of AML/CFT; employees responsible for dealing with AML/CFT issues; AML/CFT programs; awareness and education of employees, information system (transaction tracking system, traders diary); CDD procedures; detection, blocking, and reporting of unusual business transactions; counter-measures for terrorist financing; record keeping; internal audit etc. During the onsite visit supervisors conduct review of a representative sample of client files; financial transactions records (UTRs, content of UTRs, blocked transactions), verify the implementation of TFS. The private sector representative also confirmed this.

529. The number of onsite inspections (please see Table 39) performed for banks, exchange entities, securities firms and insurance appear to be insufficient. As for the payment service agents, these FIs have not been subject to AML/CFT supervision.

530. It is of a particular concern that the MVTS agents have not yet been subject to on-site supervision.

FIU

531. The authorities have not provided any information on the risk classification by the FIU of the sectors or obliged entities under its supervision. Since April 2018 the FIU instituted a risk-based approach in supervision. FIU has an annual monitoring plan according to which it carries on site investigation updated periodically if there are significant changes of the relevant circumstances. The length of the inspections conducted by the FIU depends on several factors (e.g. size of the entity supervised or complexity of the products offered) and it can take 2-3 days in case of an accountant and up to 3 months in case of banks.

532. The FIU is not conducting off-site AML/CFT supervision.

533. The FIU has 6 employees responsible for AML/CFT supervision of a large number of obliged entities. The FIU performs inspections only of the RE with high ML/FT risks, therefore only a limited number of inspections have been carried out during the period under review.

534. Although the NBS informs the FIU before conducting an onsite inspection and subsequently on the sanctions imposed, which allows to avoid duplications, there are some missing elements of effective cooperation between the two supervisory bodies. No feedback is provided by the NBS when receiving a proposal from the FIU to apply sanctions, and no joint efforts are made to assess the risk of particular FIs. FIU makes use of international cooperation with other FIUs to better inform its supervisory activities and in case relevant information is identified during the inspection it is forwarded to foreign counterpart.

Table 39: Onsite inspections conducted by the NBS and the FIU for FI's

Years	Total number of entities	Total number of onsite visits	Number of AML/CFT specific (thematic) onsite visits conducted	Number of AML/CFT combined with general supervision onsite visit carried out
Banks				
2013	28	FIU 4 NBS 8	FIU 4 NBS 1	NBS 5
2014	28	FIU 1 NBS 6	FIU 1 NBS 1	NBS 1
2015	27	FIU 1 NBS 5	FIU 1 NBS 3	NBS 1
2016	28	FIU 0 NBS 11	FIU 0 NBS 4	NBS 1
2017	26	FIU 0 NBS 9	FIU 0 NBS 4	NBS 0
2018	27	FIU 0 NBS 10	FIU 0 NBS 3	NBS 0
Securities companies				
2013	32	FIU 0 NBS 21	FIU 0 NBS 0	NBS 7
2014	34	FIU 1 NBS 29	FIU 1 NBS 0	NBS 6
2015	33	FIU 1 NBS 30	FIU 1 NBS 0	NBS 3
2016	35	FIU 0 NBS 16	FIU 0 NBS 5	NBS 2
2017	40	FIU 1 NBS 12	FIU 1 NBS 0	NBS 2
2018	41	FIU 1 NBS 12	FIU 1 NBS 0	NBS 4
Insurance companies				
2013	17+21EU	FIU 1 NBS	FIU 1 NBS 0	NBS 7

		12		
2014	17+21EU	FIU 0 NBS 15	FIU 0 NBS 0	NBS 0
2015	16+24EU	FIU 1 NBS 3	FIU 1 NBS 1	NBS 0
2016	16+23EU	FIU 0 NBS 2	FIU 0 NBS 0	NBS 0
2017	16+22EU	FIU 0 NBS 3	FIU 0 NBS 0	NBS 1
2018	14+21EU	FIU 0 NBS 6	FIU 0 NBS 2	NBS 0
Payment institutions				
2013	11	FIU 0 NBS 3	FIU 0 NBS 0	NBS 3
2014	10	FIU 1 NBS 2	FIU 1 NBS 0	NBS 2
2015	10	FIU 0 NBS 3	FIU 0 NBS 0	NBS 3
2016	11	FIU 1 NBS 3	FIU 1 NBS 0	NBS 3
2017	10	FIU 0 NBS 5	FIU 0 NBS 0	NBS 5
2018	9	FIU 1 NBS 4	FIU 1 NBS 0	NBS 4
Asset management companies				
2013	16	FIU 0	FIU 0	NBS 0
2014	11	FIU 0	FIU 0	NBS 0
2015	11	FIU 1	FIU 1	NBS 0
2016	11	FIU 0	FIU 0	NBS 0
2017	11	FIU 0	FIU 0	NBS 0
2018	11	FIU 0	FIU 0	NBS 0
Credit providers (non-banking creditors)				
2013	31	FIU 3	FIU 3	0
2014	31	FIU 3	FIU 3	0
2015	23	FIU 3	FIU 3	NBS 0
2016	32	FIU 0	FIU 0	NBS 4
2017	34	FIU 0	FIU 0	NBS 4
2018	31	FIU 3	FIU 3	NBS 4
Exchange offices				
2013	1188	FIU 1	FIU 1	NBS 10
2014	2525	FIU 1	FIU 1	NBS 9
2015	1146	FIU 1	FIU 1	NBS 11
2016	1155	FIU 0	FIU 0	NBS 0
2017	1158	FIU 1	FIU 1	NBS 0
2018	1167	FIU 0	FIU 0	NBS 12

Gambling sector

535. Until 2019 the MoF was the supervisory authority for gambling activities. Combined inspections that included AML/CFT issues have been conducted by the MoF and the Financial

Directorate before 2019, without applying a risk-based approach.[50] There was no specific AML/CFT inspection carried out.

536. The gambling sector has since June 2019 a new supervisor in GRA. At the time of the on-site visit, no AML/CFT supervision has been carried out by the latter.

Other DNFBPs

537. The FIU performed AML specific onsite inspections of DNFBPs as follows:

Table 40: Number of FIU inspections performed for the DNFBPs

Year	DNFBPs	Number of inspections
2013	Traders in precious metals and gemstones	1
	NPOs	2
	Property administration services	1
	Tax advisors	1
2014	Gambling Operators	1
	Real estate	1
	Lawyers	2
	Notaries	1
	Pawnshops	2
	NPOs	1
	Property administration services	1
	Economic consultants	1
2015	Gambling Operators	1
	Real estate	1
	Traders in precious metals and gemstones	1
	Lawyers	1
	Accountants and auditors	1
	NPOs	1
	Tax advisors	1

[50] 2013 – 3 inspections MoF; 2014 – 2 inspections MoF; 2015 – 6 inspections MoF; 2016 – 4 inspections MoF and 1 inspection Financial Directorate; 2017 – 3 inspections Financial Directorate; 2018 – 5 inspections Financial Directorate.

2016	Dealers in precious metals and stones	1
	NPOs	1
	Property administration services	1
	Tax advisors	1
2017	Tax advisors	1
2018	Notaries	1
	Property administration services	2

538. The selection of the DNFBPs subject to inspection has been done based on the information coming mainly from the UTRs. The DNFBP supervision conducted by the FIU is not fully risk-based and the FIU lacks resources for conducting effective supervisory activities.

539. Based on the overall number of inspections conducted, it can be concluded that the supervisors do not have sufficient human resources to undertake full risk-based supervision of FIs. A notable exception is the banking and insurance sectors where the number of onsite inspections conducted by the NBS during the period under consideration is sufficient. Overall, the number of onsite inspections conducted by both supervisors on REs remains low.

540. A reason for the above lack of resources is the fact that the staff of the FIU dedicated to supervision was also involved in the implementation of other tasks, such as drafting of the NRA, providing legal drafting, and interpretations of the AML/CFT Act. Therefore, the staff was not fully involved in the inspection of the obliged entities.

1.1.4. Remedial actions and effective, proportionate, and dissuasive sanctions

Sanctions

FIU

541. The FIU has a range of sanctions available to apply to its supervised entities, consisting in fines up to EUR1 000 000 natural person which are individual entrepreneurs or legal entity or EUR5 000 000 can be applied to FIs; however, the FIU does not have power to impose sanctions to natural persons which are employed by a RE. (managers/directors, compliance officers). As demonstrated under the table below, only fines have been applied by the FIU. The most frequent shortcomings identified during inspections were the following: Failure to identify the origin of funds or UBO and failure to adopt adequate measures to ensure customer's ownership and management structure; Failure to refuse to enter in a business relationship when CDD has not been conducted, Failure to submit UTRs; Failure to identify transaction without economic or legal purpose; Failure to perform ECDD that was required.

542. In addition to imposing a fine, the FIU is entitled to propose a license withdrawal. The FIU submitted once such a proposal (in January 2019) and the NBS analyzed the case in the margins of an inspection conducted. The case was still being considered by the NBS at the time of the on-site visit.

543. Since 15 March 2018, the FIU has the power to make public the final decision on the sanction. This FIU has not yet applied this power as no sanctions have been imposed based on the new legislation in force since 2018.

544. After each inspection, the FIU informs the obliged entity of the results in the form of a "notification on inspection findings", "commencement of administrative procedure on imposing a fine" and "decision on imposing a fine".

TABLE 41: AML/CFT sanctions or other remedial measures applied by the FIU

Year	Number of fines	Amount of fines (EUR)	Licence withdrawal proposal
2013	**8** (2 banks, 1 insurance company, 2 creditors, 1 exchange office, 1 real estate company, 1 person acting as organizational and economic advisor)	32 500	3
2014	**16** (1 bank, 1 broker, 1 pay company, 3 creditors, 1 exchange office, 1 trader with claims, 1 gambling games provider, 1 real estate company, 1 lawyer, 1 notary, 1 accountant, 1 pawn shop, 1 business services, 1 person acting as organizational and economic advisor)	35 800	2
2015	**13** (1 bank, 1 insurance company, 1 asset management company, 3 credit companies, 1 exchange office, 1 trader with claims, 1 gambling games provider, I precious metals and stones trader, 1 lawyer, 1 accountant, 1 person organizational and economic advisor)	37 800	0
2016	**6** (1 payment service agent, 1 auction, 1 precious metals and stones trader, 1 NPO, 1 service provider for trade companies, 1 person acting as organizational and economic advisor)	41 600	0
2017	**5** (1 securities company, 1 credit company, 1 exchange office, 1 trader with claims, 1 person acting as organisational and economic advisor)	49 200	0
2018	**5** (1 broker, 1 payment institution, 1 notary, 1 service provider for trade companies, 1 person acting as organizational and economic advisor, 1 accountant, 1 trader with claims)	39 500	0

545. The level of available sanctions in Slovak Republic is proportionate and dissuasive, however the maximum level of sanctions has never been applied and there are no sanctions for natural persons – managers or AML Officers. The level of sanctions applied by the FIU did not exceed EUR49 200. No sanctions have been applied to natural persons.

NBS

546. The imposition of sanctions by the FIU does not prejudice the ability of the sectoral supervisors to apply sanctions for AML/CFT violations. The maximum amount of fine that can be applied by the NBS according to the applicable legislation is EUR300 000 (or in case of repeated or severe violations, up to EUR600 000). The NBS informs the FIU on the shortcomings identified and sanctions applied. Unlike the FIU, the NBS can apply fines to members of the board of directors, board of supervisors, head of branch, administrator and compliance officer of an entity, but no sanction has been applied to these officials so far.

547. The most frequent AML/CFT breaches identified by the NBS were the following:

- The compliance officer did not have its duties specified in its labour contract (job description). For this deficiency was imposed a remedial action of modifying the labour contract of the compliance officer;
- There was no annual audit performed for testing the efficiency of the AML programme of the entity. The remedial action for the breach identified was that the entity draw it audit report until the end of the year and discuss it in the Supervisory Board.
- Not enough measures performed to verify the source of funds or if a transaction is suspicious or not.
- Deficiencies in conducting CDD.
- Shortcomings about independence of the designated person.

TABLE 42: Fines applied by the NBS

Year	Number of fines	Amount of fines (EUR)	Warnings	Licence withdrawals
2013	0	0	3	0
2014	1	50 000	4	0
2015	1	10 000	1	0
2016	0	0	6	0
2017	1	100 000	0	0
2018	0	0	2	0

548. The NBS applied sanctions for ML/FT related violations only in a limited number of cases. Although the NBS stated that they widely use the remedial measures, most of the interviewed FIs have not received any action plan as a result of an on-site inspection.

549. The evaluation team held meetings with the banks holding almost 65% of the banking sector and most of the bank representatives indicated that after the onsite visit by the NBS or the FIU no deficiencies have been identified and accordingly they have not been subject to any sanctioning or application of remedial measures. Considering the issues identified under IO4 the AT is concerned about the lack of remedial action plans.

550. The fines applied by the NBS to a single obliged entity never exceeded EUR100 000 and these fines are not applied only for AML/CFT breaches. Therefore, the AT considers that the sanctions applied by the NBS are not dissuasive.

Table 43: MoF- Financial Directorate of SR (Tax authority) as a supervisor of gambling sector

Year	Number of fines	Amount of fines (EUR)
2016	1	3 000
2017	3	9 000

2018	5	15 000

551. The new GRA had not yet applied any sanctions at the time of the on-site visit.

552. Taking into consideration the size of the financial and DNFBP sectors in the Slovak Republic, as well as the country risk, the sanctions applied are not dissuasive.

1.1.5. Impact of supervisory actions on compliance

553. The limited number of the on-site inspections, the low level of fines applied and the feedback from the private sector does not demonstrate that the impact of FIUs supervisory actions on the FIs and DNFBPs is significant.

554. The interviews with the private sector revealed a common understanding that in general the AML/CFT breaches identified during the onsite inspections would not lead to any significant pecuniary sanctions, provided that the obliged entity would demonstrate its willingness to remediate the shortcomings in a timely fashion.

555. While there is a positive impact on compliance mainly in stimulating the FIs to correct the breaches identified in the course of the NBSs on-site and off-site inspections, it is not clear what other actions were undertaken by supervisors to enhance compliance of FIs (such as compliance action plans). To this, the narrow sanctions and remedial measures applied by the supervisors, make the impact on compliance limited.

DNFBPs

556. The supervisor has conducted only a limited number of inspections based on the information coming mainly from the UTRs. No information (such as information on the breaches identified and sanctions applied) was provided to conclude that supervisory activities have an impact on compliance with AML/CFT obligations by the obliged entities.

1.1.6. Promoting a clear understanding of AML/CFT obligations and ML/TF risks

557. The Institute of Banking Education of the National Bank (IBV NBS) of Slovakia is conducting training for the financial sector employees. The IBV also offers e-learning programs.

558. Although the importance of such a specialized entity is acknowledged by the evaluation team, the NBS has not yet prepared or carried any trainings for the supervised entities. The NBS did not provide AML risk models or risk manuals. Nevertheless, the NBS communicates/shares information or discusses common findings from on-site and off-site supervision and international reports with the Slovak Banking Association, Slovak Insurance Association, Slovak Association of Asset Management Companies.

559. NBS has a section dedicated to AML on its website https://www.nbs.sk/en/financial-market-supervision1/supervision/prevention-of-legalisation-of-proceeds-of-criminal-activity-and-financing-of-terrorism.

560. The FIU organizes trainings for obliged persons regarding application of chosen AML/CFT Act provisions and their application in practice. While both the NBS and the FIU have undertaken some training activities, not sufficient guidance is provided to the RE on the AML/CFT risk assessment.

DNFBPs

561. The Chamber of Lawyers and the Chamber of Notaries have not issued any written guidance or training on AML/CFT matters, however they communicate via e-mail (gazette or

newsletter) to their members on AML/CFT related obligations, legal framework and practices. The FIU has provided guidance to DNFBPs on the implementation of CDD requirements, reporting of unusual transactions and designing of internal programs (for accountants, tax advisors, auditors and DPMS).

Overall conclusions on IO.3

562. The NBS has risk rated its supervised FIs using qualitative data, there is no actual and documented risk level classification, a risk map or risk matrix for each financial institution. based on the results of the NRA. The NBS has informed the evaluation team about its own risk-based methodology (not enforceable) based on which risk-based supervision is carried out. AML/CFT issues in the gambling sector have been covered to some extent during the holistic supervision conducted by the former supervisor (Ministry of Finance). As for the newly established Gambling Supervisory Authority (established in 2019), no AML/CFT inspections have been carried out yet by the latter. The NBS has in place established fitness and properness checks to prevent criminals and their associates from owning or controlling FIs, which seem adequate. Although a wide range of sanctions is available for the authorities to address violations of AML/CFT obligations, both to institutions and their management, the level of sanctions applied so far to RE cannot be considered dissuasive. Moreover, no sanctions have been applied to the management of RE.

563. **The Slovak Republic has a Moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

7.1. Key Findings and Recommended Actions

Key Findings

1. Information on the creation of all types of legal persons is publicly available in the Slovak Republic.

2. The NRA contains some analysis on the risks posed by different types of legal persons, which, however, does not amount to a sufficiently comprehensive assessment of ML/TF risks associated with all types of legal persons. On a positive note, there is a clear understanding among all authorities that mostly LLCs are being misused for ML/TF purposes.

3. The LEAs, the FIU and the banks identified risks and took proactive mitigation measures in relation to *"virtual seats"* of legal persons and the use of *"straw men"* in corporate structures. The other supervisors do not have sufficient understanding on this phenomenon.

4. Basic information on legal persons is contained in relevant registers. All competent authorities, including the supervisors, the LEAs and the FIU have direct access to all registers. The AT did not identify any issue on the accuracy of basic information during the on-site visit.

5. Slovakia has created the *"Register of legal entities, entrepreneurs and public authorities"* (hereafter the UBO register) in 2018, which was in train on being populated. At the time of onsite, only 12 % of legal persons inserted their UBO data into the UBO register, and the filling progressively continues. There are no mechanisms in place to verify the information on the UBOs at the time of registration. In the meantime, some control mechanisms are done *ex post* by state authorities, such as LEAs, tax authorities, as well as by media and NGOs.

6. Besides the UBO register, the Register of Public Partners also contains information on UBOs of legal entities involved in any public contract relationships. The state authorities and private sector consider the data contained in this register as high quality. Although there is a system of verification, the UBO information is mainly identified and verified by some DNFBPs who have a formal and limited understanding of UBO.

7. The LEAs obtain UBO data from FIs (mostly banks). Although LEAs consider this information to be trustworthy, the shortcomings related to the understanding of UBO by some banks to some extent underpins the quality of the obtained information.

8. Bearer shares are *de facto* prohibited in Slovakia, since they can only be issued in the form of book-entry securities and are registered with the Central Securities Depository.

9. Legal arrangements are not recognized in Slovakia, but their activity is not prohibited elsewhere. Based on the interviews with state authorities and private sector, the AT concludes that there are no legal arrangements operating in Slovakia.

10. No sanctions were imposed for submitting inaccurate UBO information, as the register was not complete at the time of onsite visit. Sanctions on legal persons related to the submission of inaccurate basic information or failure to submit such information in a timely manner have been applied in a limited number of cases.

Recommended Actions

Authorities should:

1. Carry out a comprehensive analysis of risks associated with all types of legal entities and ensure the awareness of all stakeholders and RE on the risks identified and respective mitigating measures to be taken. The analysis should, inter alia, take into account risks identified with *"virtual seats"* of legal persons and *"straw men"* used in corporate structures, percentage of foreign involvement of such cases.

2. Ensure that the understanding of the notion of the UBO among the public and private sectors is in line with the requirements of IO5.

3. Ensure that all registers have adequate resources and legal powers to hold accurate and up-to-date beneficial ownership information. Adequate verification mechanisms to ensure the information contained in the registers is accurate and up to date should be introduced. The relevant authorities should receive training on the characteristics of legal arrangements, their potential misuse and on ways of obtaining information on the, including through international cooperation.

4. Slovakia should apply proportionate and dissuasive sanctions where violations are identified and maintain statistics on the type and number of sanctions imposed on legal persons for breaching basic or beneficial ownership registration regimes.

564. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this section are R.24-25.[51]

7.2. Immediate Outcome 5 (Legal Persons and Arrangements)

565. By way of context and materiality, it should be noted that Slovakia is not a company formation center. No specific benefits (e.g. reduced corporate tax rates or exemptions) are offered to non-residents wishing to set up companies in Slovakia. It is not common to set up companies as part of complex corporate structures (e.g. as a holding company). Slovakia is not a member to Hague convention of 1 July 1985 on the Law Applicable to Trusts and on their Recognition and does not recognize or regulate the creation of legal arrangements, such as trusts. According to the interviews there are no business relationships with foreign trusts either.

566. The authorities have limited understanding on basic characteristics of legal arrangements and ways of obtaining information on them. The ML/TF risks posed by the legal arrangements have not been assessed. The private sector, mainly larger banks, demonstrated sufficient understanding of ML/TF risks related to legal arrangements and stated that they do not have such clients.

567. The Slovakia`s legal framework provides for the establishment of the following legal persons: limited liability companies, joint stock companies, simple joint stock companies, unlimited partnership, limited partnership, cooperative, associations, non-profit organizations, non-investment funds and foundations.

[51] The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

568. As at the end of 2018, there was a total of 330 336 registered legal persons in 11 different legal forms, with the most common types being limited liability companies (262 218), associations (46 859), joint stock companies (7 367). Legal persons registered in Slovakia are mostly owned by the residents of the Slovak Republic (only about 7% of legal entities have foreign ownership).

569. Limited liability companies are by far the most common form of legal persons involved in ML and criminal schemes, based on statistics and data gathered from LEAs and supervisory authorities.

7.2.1. Public availability of information on the creation and types of legal persons and arrangements

570. As noted in more detail at R.24, information on the various types, forms and basic features of Slovakian legal persons is publicly available and provided in the relevant pieces of legislation, such as the Commercial Code, the Civil Code, the Law on Foundations (No. 34/2002), the Law on Non-Profit Organizations Providing Generally Useful Services (No. 213/1997), the Law on Non-Investment Funds (No. 147/1997) and the Law on Slovak National Council (No. 207/1996). Besides, various types, forms and basic features of business enterprises are contained in the website provided by the Government of the Republic of Slovakia (https://www.slovensko.sk/sk/titulna-stranka).

7.2.2. Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal entities

571. The NRA analyzes the ML/TF vulnerability of FIs and DNFBPs, as well as TF vulnerability of foundations, non-profit organizations and non-investment funds. However, this does not amount to a sufficiently comprehensive assessment of ML/TF risks stemming from the characteristics, nature and scope of activities of various types of legal persons that exist in the country. This analysis is mainly based on the effectiveness of implementation of preventive measures by the RE in case of legal entities, rather than cases of misuse of legal persons for ML/TF purposes identified domestically.

572. While the country has not gone through the motions of identifying and assessing the risks posed by the totality of legal persons, there is a common understanding among competent authorities that limited liability companies are most common form of legal persons abused in terms of ML and for wider criminal purposes due to the fact that this is also the most common type of legal persons.

573. The main risks were identified with regard to *"virtual seats"* of these persons and the use of *"straw men"* in corporate structures. The understanding of this risk amongst Police, FIU and GPO is satisfactory and emerges from through their operational activities. Companies with *"virtual seats"* are understood as legal entities usually registerred in one address, but with no activity (similar to shell companies).

574. The FIU conducted an analysis which revealed about 800 legal persons registered in one single address. Mitigating measures are being taken, as explained under core issue 5.3, to thwart this problem. However, despite the efforts, the scale of this phenomenon is not sufficiently explored, and a more comprehensive analysis is needed. For instance, there are indications that the *"virtual seats"* are also misused by non-residents but the extent to which this happens is not known. As opposed to the LEAs and the FIU, other competent authorities, particularly supervisors, have more limited understanding of the above-mentioned phenomenon.

575. The concept of *"straw men"* is widely understood as, a homeless man, who is registered as a director of a legal entity without any further involvement in the business activity. As opposed to *"virtual seats"*, authorities stated that non-residents are not involved in such structures. However, no formal analysis considering all possible aspects of involvement of non-residents (for e.g. in the ownership structure) was conducted.

576. The private sector is not properly informed on the ML/TF risks and vulnerabilities of legal entities. Within the RE only banks have some understanding on the phenomena of *"virtual seats"* of legal persons and the use of *"straw men"* in corporate structures, who were able to describe cases of UTRs filed to the FIU on business relationships involving such customers.

577. According to the authorities, other forms of ML risks the legal persons are exposed to relate mostly to tax evasion and corruption crimes.

7.2.3. Mitigating measures to prevent the misuse of legal persons and arrangements

578. All types of legal persons must be registered through different registries to be considered as operational. The Commercial Register, which is maintained by 8 Register courts holds basic and shareholder information on trade companies and cooperatives, except for the joint stock companies (whether public or private) and simple joint stock companies: limited liability companies, unlimited partnership, limited partnership, cooperatives. In case a joint stock company or a simple joint stock company is owned by a sole shareholder, such shareholder will be registered with the Commercial Register, otherwise the shareholders are registered with the Central Securities Depositary. The Register of NPOs and the Register of Foundations contains information on founders and members of statutory bodies of NPOs and foundations.

579. There are some measures in place for verification of basic information, particularly with regard to the Commercial Register. The Commercial Registry makes several (altogether 19) checks with other State-managed registries (such as the Registry of natural persons, Registry of addresses, Registry of misdemeanours, Registry of distraints (enforcement proceedings), Registry of debtors of the Social Security, Registry of motor vehicles, Tax Registry, Registry of disqualification, etc.). Some of these checks are made automatically, others (such as disqualification) are done manually.

580. Neither the authorities, nor the private sector representatives mentioned complaints with regard to the quality and accuracy of the basic information contained in the registers, which may be due to the fact that submitting basic information to the registries is the only way a legal entity can exercise legal powers (*e.g*. engaging in a contract). The AT did not identify any issue on the accuracy of basic information during the on-site visit.

581. Another important mitigating measure was the establishment of the Disqualification Register within the Žilina District Court in 2016, which is keeps a list of disqualified natural persons (mainly individuals acting in the past as *"straw men"*). The Žilina District Court also solves disputes related to any inaccuracies found in the basic information contained in the Register of Public Partners. However, the Žilina District Court does not conduct regular checks of the records. Discrepancies in records are advised to the Register Court when identified by state authorities, such as LEAs, tax authorities, and by media and NGOs.

582. The Žilina District Court`s is responsible for checking the information related to the management of legal persons. In case of suspicions about the identity of the director (in terms of being a *"straw men"*) he/she is automatically deleted from the Register as owner of manager, and he/she is listed as a disqualified person in the Disqualification Register. The most common way of

getting informed about potentially suspicious individuals (acting as *"straw men"* in coming from the FI and LEA operational analysis.

583. There have been 220 disqualifications since 2015, which were mainly related to identified *"straw men"* within company structures/management. The MoJ publishes the list of disqualifications on its website, which is widely used by banks in the CDD processes.

584. An important mitigating measure with regard to the legal persons having *"virtual seats"* is the analysis conducted by the FIU, the results of which were disseminated to the RE. This analysis is widely used by banks, which reject /terminate business relationship with entities there included, and file UTRs on such legal persons.

585. LEAs demonstrated good awareness on the phenomenon of *"straw man"* and try to proactively identify the UBO behind each legal entity somehow involved in a criminal case through operative intelligence and other means, such as requesting information from different registries and RE.

586. In 2018 Slovakia established the UBO register as a centralized register for all types of legal persons (except for churches, religious societies and certain types of civic associations). The legal entities may file their UBO information to the register until December 31, 2019, and the time of the onsite visit, only 12% of legal entities have submitted relevant information. The data in the Register of BO shall be deemed to be complete and relevant until proven otherwise. There are no legal gateways for the register to verify the accuracy of the BO information submitted.

587. Besides the legal gateways, the AT also has concerns on the capacity of the Registers to conduct verification of the BO information with the current resources.

588. The Register of Public Partners also contains information on UBOs of legal entities involved in public contract relationship. The state authorities and private sector representatives mentioned that the data contained in this register is of a high quality. However, as the main source for UBO identification, this contains information for a limited share of legal entities registered in Slovakia (app. 19 000 legal entities out of 330 336). The LEAs also widely use BO information obtained by banks.

589. Bearer shares can only be issued in the form of book-entry securities and are registered with the Central Securities Depository thus allowing effective identification of the owners of the bearer shares.

590. Although Slovakia does not provide for the concept of nominees, the phenomena of using a "straw man" in company structures is very similar to the concept of nominee directors and is acknowledged by authorities.

7.2.4. Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons/arrangements

591. Competent authorities and RE may obtain basic and BO information on legal persons from the respective registers (the Commercial Register, the Register of Public Partners, the Register of NPOs and the Register of Foundations) which are publicly available.

592. As mentioned above, at the time of onsite visit the UBO register included UBO information only about 12% of legal entities. There are no mechanisms to verify the accuracy and currency of the information included in the UBO registry. The quality of data mostly depends on the diligence of the registered entity and changes are only based on notifications by the entity. Therefore, there is a serious concern on how the UBOs information will be verified.

593. Turning to the Registry of Public Partners, which also contains UBO data, it is important to mention that although there is a mechanism of verification, particularly, through lawyers, notaries, auditors or tax advisors, the quality of the UBO data is still questionable, since most of these DNFBPs mentioned have very formal and limited understanding of the UBO concept and identification.

594. The main sources of UBO information for LEAs and the FIU are the banks. Although legal persons are not formally required to open a bank account in Slovakia, *de facto* they do so in practice. Reportedly, there are no difficulties in obtaining UBO information, and no cases of a legal entity registered in Slovakia not having a bank account. The information kept by the banks is generally adequate, accurate, current and provided promptly, within the stipulated timeframes. LEAs consider this information to be trustworthy and it is widely used it in the investigations. However, as mentioned IO 4, the understanding of the UBO definition varies throughout the banking sector and therefore, the shortcomings related to the UBO to some extent underpins the quality of the information. Another mechanism is the UBO information held by the legal person itself. The effectiveness of this provision could not be assessed since none of the interviewed state authorities used this source of information in practice.

595. It According to the authorities and private sector representatives there are no foreign legal arrangements operating in the country. While it is not prohibited to manage legal arrangements by persons resident in the jurisdiction, in practice this appears to not be happening. What concerns existing legal mechanisms for basic and BO information on legal arrangements please refer to R.25.

7.2.6. Effectiveness, proportionality and dissuasiveness of sanctions

596. The registration court may sanction a natural person entitled to act on behalf of a registered legal entity with a fine of up to EUR3 310 if the person fails to perform the obligations related to updating information or provides false or outdated information. Besides, the FIU is entitled to impose a fine on a legal entity up to EUR200 000 for failure to fulfill the obligation to retain information related to the UBO by the legal entity according to the AML/CFT Act. Sanctions on legal persons related to the submission of inaccurate basic information or failure to submit such information in a timely manner have been applied in a limited number of cases (fines up to EUR 125 have been applied). Thus, the evaluators could not conclude that available sanctions proved effective, proportionate and dissuasive.

597. No fines have been imposed on RE for failure to identify the BO of the customer. Thus, the AT could not conclude whether available sanctions proved effective, proportionate and dissuasive. The absence of any sanctions applied indicates that proactive monitoring is not conducted neither by the FIU, nor the registration courts.

Overall conclusions on IO.5

598. The LEAs, the FIU and the banks identified and understood the risks in relation to *"virtual seats"* of legal persons and the use of *"straw men"* in corporate structures. Proactive mitigation measures were taken. The supervisors do not have sufficient understanding on this phenomenon. Information on the creation of all types of legal persons is publicly available in the Slovak Republic. Slovakia has created the UBO register in 2018 which, at the time of the on-site visit was in train on being populated with only 12 % of legal persons having submitted the UBO information. There are no mechanisms in place to verify the information on the UBOs at the time of registration. The LEAs obtain UBO data from FIs (mostly banks). Although LEAs consider this information to be trustworthy, the shortcomings related to the definition of UBO to some extent underpins the quality of the obtained information. **Slovakia has achieved a Moderate level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL COOPERATION

8.1. Key Findings and Recommended Actions

Key Findings

1. Authorities of the Slovak Republic have generally been active in providing MLA in relation to foreign requests in a constructive and timely manner, which also goes for requests related to the seizure of property as well as the participation in numerous JITs. Most of the requests are received and executed in direct (mainly EU-based) cooperation with foreign counterparts, with frequent involvement of the EUROJUST if necessary.

2. While the extradition regime has been performing satisfactorily, the Slovak Republic could not demonstrate that domestic procedures are systematically initiated, upon the request of the respective foreign country, in cases where the extradition of a Slovak national has been refused.

3. The authorities were active in requesting MLA – although while every foreign elements of a criminal case must be supported by evidence obtained from abroad, there seems to be no practical mechanism to avoid requesting assistance from abroad (and thus to avoid the potential delays).

4. The FIU cooperates with its counterparts in a generally proactive and constructive manner, both spontaneously and upon request. A portion of the latter seem to have been generated in ML cases, until recently, by the relatively high evidentiary demands of the LEA. The LEA are equally engaged in frequent and constructive cooperation with their counterparts also at the operational level.

Recommended Actions

1. The Slovak authorities should ensure that the non-execution of incoming extradition requests is effectively followed by domestic procedures whenever so requested by the respective foreign jurisdiction.

2. In order to avoid unnecessary delays caused by mechanistically seeking for MLA from abroad in cases with foreign elements, the authorities should explore practical mechanism to maximize the use of other evidence available domestically.

599. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this section are R.36-40.

8.2. Immediate Outcome 2 (International Cooperation)

8.2.1. Providing constructive and timely MLA and extradition

600. The regime for providing mutual legal assistance in criminal matters is a comprehensive legal framework described in details in the TCA that gives precedence, wherever applicable, to EU legal instruments as well as bi- and multilateral agreements providing for more simple and effective mechanism with direct cooperation between counterpart authorities. As the majority of incoming (and outgoing) requests concern other EU Member States, the importance of mechanisms such as the European Investigation Order (EIO) and European Arrest Warrant (EAW) is essential.

Table 44: Judicial Cooperation – Prosecution Service

INCOMING REQUESTS for LEGAL ASSISTANCE			
	ALL **total/direct legal contact**	**ML** **total/direct legal contact**	**FT** **total/direct legal contact**
Received	**2013**		
	2 533/2 072	28/20	0
	2014		
	2 768/2 406	36/24	0
	2015		
	3 182/2799	52/38	0
	2016		
	3 492/3 050	62/34	0
	2017		
	4 057/3 247	95/76	0
	2018		
	2 822/2 544	121/107	2
	2013-2018		
	18 854/16 118	394/299	2

601. Out of the total 18 854 requests for legal assistance in the pre-trial stage (including EIOs) delivered during the evaluated period, about 85 % were received in direct legal contact or without intervention of the GPO as a central judicial authority. The total number of requests, in which criminal prosecution was conducted for ML is 394, of which 147 requests were sent directly to district or regional prosecutor's offices.

602. The volume of incoming requests increased every year up until 2017 (2 533 to 4 057) with a nominal decrease in 2018 (4 057 to 2 822) which might have been related to the introduction of the EIO as a new instrument between EU member states. Despite the decrease in total figures in 2018, the Slovak authorities have not noticed any significant changes as regards the scope of acts requested in this year. In contrast to the trend mentioned above, the number of foreign requests with the ML element show a steady growth throughout the assessed period despite the 2018 decrease in the total figures.

603. More information on the incoming requests can be seen in the following table, which is an excerpt of a more detailed table, focusing at countries which most often submitted letters rogatory or EIOs to the Slovak Republic either in general terms or specifically in ML cases.

Table 45: Prosecution Service – MLA provided

INCOMING REQUESTS * EXCERPT *														
	2013		**2014**		**2015**		**2016**		**2017**		**2018**		**2013-2018**	
	All	**ML**	**All**	**ML**	**All**	**ML**	**All**	**ML**	**All**	**ML**	**All**	**ML**	**All**	**ML***
BE	17	2/0	17				43	3/1	42	9/0	4	1/0	123	15/1
BG			8		8		30		27	1/0	18	3/0	91	4/0
CZ	1 402	16/16	1 436	16/16	1611	22/22	1 821	20/20	1 837	38/37	1 373	36/36	9 480	148/147
FR	19		15	2/0	30	2/0	41	10/1	18	1/0	3	3/3	126	18/4
LV	1	1/0	3		3		15	3/0	10	2/0		1/0	32	7/0
LIE				2/0					4	1/0	3	1/0	7	4/0
HU	425		460		460	4/4	356	1/0	371	7/7	109	28/28	2 181	40/39
PL	190	3/3	253	4/4	338	10/10	290	9/9	431	29/28	175	24/24	1 677	79/78
AT	152		148		228		366	2/2	733	4/4	848	4/4	2 475	10/10
RO	30		23	1/0	32	2/0	64		37	1/0	20	4/0	206	8/0
GE	183	4/1	153	4/2	233	6/0	246	4/0	234	1/0	79	5/0	1 128	24/3
UK	23		15	3/0	11		9		17		10		85	3/0

SRB	16		11	1/0	6	1/0	2		1				36	2/0
SUI	11	1/0	20		29		38	5/0	41		19	1/1	158	7/1
IT	24	1/0	12		13	1/0	16	3/1	25		3	6/1	93	11/2

*ML: Central authority/direct contact (regional and district prosecutor's offices)

604. MLA requests are mainly received from EU countries, in particular from the neighboring EU Member States (CZ, AT, HU, PL) out of which the Czech Republic has submitted approximately half of all incoming requests alone, thereby reflecting the economic and social relations of the SR. On the other hand, hardly any requests were received from the non-EU neighbor Ukraine (75 requests in 5 years with only 1 relating to ML).

605. The scope of requested acts of legal assistance can be seen in the following table. Again, this is an excerpt from a more detailed table, reduced to the most important figures for the years 2016-2018 (an IT case management system called PTCA, which allows for breaking down statistical figures in such details, was only introduced in 2016).

Table 46: MLA provided (excerpts)

Type of act	2016	2017	2018
Documentary evidence	646	629	565
Bank data (representing bank secret)	769	829	646
Delivery	521	781	1 175
Identification of person	132	203	180
Interrogation	2 233	2 257	1 996
Video conferences	10	19	20
Seizure of financial resources	28	16	19
Seizure of property	6	1	4
Seizure of evidence	8	11	5
Search /home, other premises)	26	36	30
Procedure according to Act No. 650/2005 Coll.		1	3
Cross-border surveillance and pursuit	13	14	13
Surveillance of people and things	5	7	6
Video, audio, and audio-video records	5	6	13
Wiretapping and recording of telecommunication operation	7	2	4
Obtaining and provision of data on telecommunication operation	48	50	51
Content computer data	4	12	7
Operating computer data	48	72	33
Tax data (data representing tax secret)	36	58	51
Business data (data representing business secret)	8	4	8

606. Subject matters of requests were in most of the cases traditional investigative acts (production and delivery of documents, hearing of defendants or witnesses etc.) with only a few (although increasing number of) cases involving various property-related coercive measures, predominantly from EU countries. Special investigative measures have also been asked for and carried out in a regulate manner.

607. The investigative acts most frequently requested by foreign states in connection with ML offences were the provision of banking data and documents, other documentary evidence including copies of file materials from domestic proceedings, and hearing of witnesses. In other cases, search was performed in the premises of companies and accounting documents were seized upon the request of a foreign country.

608. As regards the length of performance of legal assistance acts, it varies depending on the required acts. The total average period for executing foreign requests throughout the period 2013 to 2018 was about 2 months (63 days) while specifically in ML-related cases the average time for

execution was slightly longer (considering the characteristics of the requested investigative acts) as follows:

Table 47: Average time for executing ML-related MLA requests

Year	Average Time
2013	101 days
2014	65 days
2015	80 days
2016	88 days
2017	77 days
2018	83 days

609. As it was explained by the authorities, most of the requests are executed within a shorter period (*e.g.* simple request consisting of provision of banking data are dealt with in one month) but other cases may last as long as 6 months due to specific reasons such as unavailability of witnesses or difficulties in obtaining documentary evidence. In most cases, however, when the execution exceeded 4 months it was at least partly affected by technical deficiencies on the requesting side (such as incomplete requests, missing annexes etc.). As an illustration to that, Slovak authorities provided the following example for the timely execution of a foreign request in a complex case:

CASE BOX 13: The "Hackers" case

The Regional Prosecutor's Office Žilina (RPO Žilina) received a request from the prosecutor's office in Rotterdam (NL) on 16.02.2018 related to a criminal case of extortion (blackmail). According to the request, a group of hackers (employees or former employees of a Dutch telecommunications company, including a Slovakian and a Dutch citizen) sent several digital messages to the said company through the customer website from January 2018 and the latest on 13.02.2018. The perpetrators claimed to have access to personal data of customers (which they corroborated by a "sample" of stolen data) and demanded a payment in bitcoins as a consideration for preventing the publication of such information or sharing it with the customers.

The Dutch request was aimed at capturing the Slovakian perpetrator (simultaneously with the arrest of the Dutch perpetrator in the Netherlands) and providing evidence, including the localisation of the suspect, the search of his apartment for evidence, the seizure of such items (e.g. computers and other IT equipment, mobile phones, data carriers) and the administration of bitcoins or other cryptocurrencies. With respect to the character of the cybercrime, the European Judicial Cybercrime Network was also involved.

This was a very urgent situation, because while the request for cooperation was sent to the EJN contact point of the Slovak Republic on Friday 16.02.2018, the latest date for an action was 20.02.2018 as the data of the customers would have been disclosed no later than on 21.02.2018 if the amount had not been paid. It was therefore important that the NL contact point provided adequate information on the factual circumstances and the urgency of the case as from the beginning.

The EJN contact points had intensive communication about the cooperation, including issues to be dealt with by police authorities (the software used, the method of communication of the offenders, covert inspection of the site, etc.), as well as by judicial authorities (determination of competence, the documents needed from the NL, the presence of investigators from the NL when performing acts in the territory of the SR, a preliminary agreement on performing the acts in parallel in the NL and SR). After that, it was determined

that the RPO Žilina had competence for the execution of the request, so this office was contacted. The prosecutor was provided with all contact information and communicated with the police department of cybercrime. Eventually it was determined that issuing an EAW and an EIO by the Dutch authorities would be necessary for the requested acts, depending on the results of the ongoing police operations for localising the perpetrator. The Dutch prosecutor prepared the draft EIO by Saturday 17.02.2018 and the EAW was also in preparation. On 19.02.2018 the SR authorities confirmed that they were ready to perform the acts if both the EIO and EAW were sent. The NL contact point sent the draft EIO (without translation, presumably in English) so that the requested acts can be prepared in time, while requirements for sending the EIO in Slovakian translation were explained to the Dutch part. At this stage, direct contact data at the RPO Žilina were provided to the Dutch part so that they could discuss certain specific details (e.g. in relation to the presence of Dutch investigators during the acts) Finally, all the acts were carried out in both countries on 20.02.2018. A search of the home was carried out, the person was detained, data were seized. The detainee cooperated and provided the necessary access data. After performing the acts, the competent authorities informed each other and also the EJCN contact points of both countries were informed (in the meantime, the Dutch perpetrator was also apprehended in the Netherlands). The Slovak offender was extradited to the Netherlands based on the EAW.

610. In accordance with the findings under R.37 in the TCA, the assessors were not informed of any special facts that would create obstacles in providing effective judicial cooperation. As regards foreign requests refused or not executed (the number of which was reported to be negligible such as 2-4% maximum) the only examples the Slovakian authorities provided were related to objective technical reasons (such cancellation of the bank account regarding which seizure was requested, the unavailability of a witness, the expiry of the period for saving data by mobile phone operators) or the failure of the requesting authority to provide additional information (the case examples provided appear to demonstrate, however, the efforts of Slovak prosecutors to ask for such information whenever possible). The dual criminality standard only applies to procedural acts the performance of which requires a court order (see R.37) in which area, however, its application has reportedly been an obstacle, in rare cases, to provide legal assistance.

611. As it was expressed by the GPO, the Slovakian authorities has granted all requests of foreign judicial authorities for the presence of their investigators or prosecutors at the legal assistance acts performed in the SR. Such actions took place with regularity throughout the assessed period, with 74 to 156 cases per year, involving representatives mostly from the neighboring countries who participated particularly in hearings of witnesses and searches of homes and non-residential premises.

612. As far as prioritization is concerned, the requests for legal assistance have priority if urgency is justified by any circumstances, such as in cases where the person is prosecuted in custody or if it results from the request that its execution does not bear any delay and fast action is needed *(e.g.* for fast performance of a search and seizure, performance of any acts by the date of a scheduled court hearing etc.) The requests for obtaining and notifying data on telecommunication operation also have priority, due to a possible expiry of time-limit for data holding. If the requesting authority asks for fast response to the request also for other reasons, the responding prosecutor's office always tries to comply and perform acts in any criminal matter properly and in time. Prioritization is assisted by the case management system PTCA used by the Prosecution Service which contains each incoming request in electronic format that allows monitoring the responses, and in which requests related to ML/FT offences and/or to seizure of proceeds of crime are automatically given priority pursuant to a formal instruction issued by the GPO in May 2018. A

similar system (Fabasoft) has been installed at the MoJ the performance of which has some apparent issues (see the deficient data regarding the extradition/EAW regime).

613. Timely performance is based on the specialisation of prosecutors for the area of judicial cooperation and existence of 24/7 emergency system of prosecutors and judges for pre-trial proceedings. Urgent requests can be sent in electronic form through EUROJUST complemented by EJN contact points and channels for police cooperation (SIRENE, Interpol). It is noted as an issue of effectiveness that the Slovak Republic implemented the EIO by requiring that it can only be submitted, even in urgent cases, in Slovakian (or for EIOs coming from the Czech Republic, also Czech language), which requirement would normally apply also to EIOs sent via EUROJUST. Considering the unavoidable delays caused by the translation, several EU member states have declared to accept EIOs also in English (and/or other vehicular language) instead of their respective official languages, at least on the condition of reciprocity and in cases of extreme urgency – which, in case of Slovakia, may only apply, on an informal case-by-case basis, to some urgent EIOs either accepted in draft before being translated (see the "Hackers" case above) or sent through the EUROJUST.

CASE BOX 14: A comprehensive case with a combination of EAW and EIO

The Regional Prosecutor's Office Košice (RPO Košice) executed an EIO that had been issued by the competent Italian prosecutorial authority in relation to an Italian citizen who had previously been surrendered by Slovakia to Italy on the basis of an EAW issued by the competent Italian court.

The person was sought by Italy to be prosecuted for the criminal offences of association for purposes of illicit traffic in narcotic drugs and psychotropic substances committed by an organised criminal group as well as money laundering. Having him arrested in Slovakia in March 2018, the RPO Košice performed preliminary investigation about the Italian EAW as a result of which the RPO Košice issued a resolution on the execution of this EAW and the requested person was surrendered to Italy for being prosecuted.

During this procedure, the RPO Košice was delivered an EIO issued in April 2018 by the competent Italian prosecutorial authority relating to the criminal procedure conducted in the Italian Republic against the aforementioned Italian citizen. The Italian party requested the execution of investigation measures leading to detection and identification of movable and immovable assets, financial relations, working activity, obtained and admitted income, business activity, public documents containing property-related and financial data, all that in relation to the accused Italian citizen, his wife and accomplices, and the detection and identification of owners of 144 phone numbers.

Due to the extensiveness of requested data, the RPO Košice asked its Italian counterpart for additional information, and due to the seriousness of the matter, the EUROJUST was also involved to enhance the cooperation. The EIO was executed in parts and evidence was submitted to the Italian authorities in 2019.

614. The MoJ is the central authority for courts in the area of judicial cooperation and thus it provides professional and coordination support to courts in this respect. As far as incoming requests are concerned, these are generally dealt with by District Prosecutor's Offices regardless of the stage of criminal proceedings and will only be handled by a court if so, requested by the foreign judicial authority. While in case of EU Member States, such requests are communicated directly between judicial authorities, the MoJ remains involved in sending and receiving letters rogatory to and from other countries (out of which requests related to cases in pre-trial stage are then forwarded to the competent District PO). The AT was left without proper and detailed statistics in this regard. For the period 2013 to 2017 the MoJ could only provide annual cumulative numbers of incoming and outgoing letters rogatory, with the following figures.

Table 48: Incoming and outgoing letters rogatory

Year	Total
2013	86
2014	87
2015	99
2016	90
2017	139

615. In 2018, the MoJ received 78 foreign letters rogatory which were dealt with as follows. The countries most actively asking for legal assistance in court cases were the neighboring EU member states (CZ, AT, HU) and the United Kingdom. However, the majority of these cases were related to cases still in pre-trial phase and thus forwarded to the GPO (and therefore counted in the respective GPO statistics too).

Table 49: Foreign letters rogatory

Status	Total
Received (passive)	78
Settled	43
Pending	24
Refused	11

616. Slovakian prosecutorial authorities demonstrated their capability and willingness in taking over criminal prosecutions from abroad as well as accepting criminal complaints from other countries. The number of such cases throughout the assessed period can be seen in the following, redacted statistics:

Table 50: Criminal prosecutions triggered from international assistance requests

Year	CRIMINAL PROSECUTION TAKEN OVER FROM ABROAD Total/Competence of Reg.Pros.Office	RECEIVED CRIMINAL COMPLAINTS FROM FOREIGN COUNTRY Total/Competence of Reg.Pros.Office	Total
2013	104/7	508/7	**612/14**
2014	104/7	454/338	**558/345**
2015	93	422/326	**526/326**
2016	43	534/357	**577/357**
2017	78/63	531/456	**609/519**
2018	45/9	477/434	**522/443**

617. In the table above, the taken over proceedings involved citizens of the SR having committed criminal offences abroad. These cases, as well as the criminal complaints received from abroad, were mostly related to crimes against property, however in some cases ML offences were also represented. The majority of the countries involved were, as usual, the neighbors of the SR with cases predominantly from the Czech Republic. ML-related proceedings taken over and criminal complaints accepted in most cases reflected the situations where the predicate crime and the associated ML offence took place in different countries so this mechanism proved effective in avoiding duplication of proceedings or conflicts of jurisdiction. Such cases are summarized in the following table.

Table 51: Criminal proceedings

Year	Proceedings taken over (ML)	Criminal complaints (ML)
2013	1 (CZ)	2 (CZ)
2014		8 (CZ/4 DE/1 other/3)
2015	1 (CZ)	9 (CZ/2 AT/2 other/5)
2016	3 (CZ/AT/HU)	3 (AT/2 DE/1)

2017		9 (CZ/2 FR/2 other/6)
2018	1 (HU)	12 (DE/3 CZ/2 other/7)

618. Slovakia has demonstrated its capability to establish and to participate in Joint Investigative Teams (JIT) with other EU Member States. In the first part of the assessed period, Slovakian authorities entered into 2-3 such JITs annually, but there was a significant increase in the years 2017 and 2018 with 7 JITs established each year, as a result of which the Slovak Republic was actively operating in 23 JITs at the beginning of 2019. Most of these JITs involved neighbouring EU countries (predominantly the Czech Republic) but in one case a non-EU country (Serbia) did also participate, which shows the ability of the judicial authorities to establish JIT also on the basis of reciprocity. The majority of the JITs were related to drug related crimes (7 cases mostly with the Czech Republic) tax related crimes (7 cases with the Czech Republic) and trafficking in human beings (3 cases with UK).

619. As most of these JITs target proceeds-generating crimes, the assessors welcome that a growing number of JITs have also been extended to associated ML offences. A JIT targeting an OCG involved in tax crimes and ML was established in 2013 (CZ) there were 2 others in relation to ML associated with trafficking in human beings (both UK) another one in 2018 where ML was associated with environmental crimes (HU) and a fifth JIT was set up in 2017 targeting fraud and associated ML offences (CZ).

CASE BOX 15 – Examples of JITs concluded in ML related cases

JIT "Operation Robotic"

The JIT agreement was concluded with UK in 2017 in relation to criminal proceedings conducted in both countries, for human trafficking and a particularly serious crime of money laundering. The factual basis is that members of an OCG have been transferring persons, who had been living in unfavourable social conditions in Slovakia, to the UK by promising them a financially profitable job. After arrival, the victims were made to work 12-14 hours a day, six days a week for 20£ a week and the money they earned was obtained and transferred to the Slovak Republic by the members of the said OVG. Within the JIT, a financial investigation was carried out in the Slovak Republic, interceptions were made, house searches, interviews of witnesses were carried out and document evidence was provided.

JIT in case of suspect J.K. et al.

The IT agreement was concluded with the Czech Republic in 2017 in relation to criminal proceedings conducted only in the Czech Republic for the offences of fraud and money laundering. The factual basis is that the suspect, as the manager of companies residing in the USA, was offering for sale an automatic trading system. A part of the payment for the purchase of this automatic trading system was the license fee, while the other part was fraudulently promised to be invested to trading on Forex and commodity markets. The perpetrator, however, did not invest this second part of the payments as promised but used it for his own purposes such as to finance the operation of other companies as well as to purchase real estate and other companies. Within the JIT, interviews of witnesses were carried out and information on bank accounts and companies operating in the territory of the Slovak Republic was provided.

620. As discussed more in details in the TCA, foreign confiscation orders can be executed in the Slovak Republic through the general CCP mechanism applicable for recognition and enforcement of foreign court decisions, provided that there is a bilateral or multilateral treaty basis and that the foreign judgment, which pronounced the confiscation measure, has previously been recognized by

a domestic court order. The evaluators learnt that during the assessed period, no foreign requests were received and processed according to this legal framework.

621. In relation to other EU member states, foreign confiscation orders are recognized and executed in a certificate mechanism introduced by Council Framework Decision 2006/783/JHA (implemented by Act 316/2016 Coll. on the recognition and enforcement of property-related decisions issued in criminal proceedings) in which regime the MoJ is competent for receiving and sending of certificates, as well as for determining the competent Slovakian judicial authority or informing the foreign authority thereof, but in course of the proceedings, the courts communicate directly with the judicial authorities of Member States. Since the introduction of this mechanism in 2017 there have been 4 requests received: 2 cases in 2017 from Italy (related to ML and fraud cases) and 2 cases in 2018 from Slovenia (related to theft). All 4 cases are still pending before the competent courts. The description of the respective cases prove that the delay was caused by technical reasons (discrepancy between the certificate and the underlying documents, lack of translation or supporting documents) and, in one of the cases, also a competency dispute between the civil and criminal section of the competent court.

622. Execution of foreign requests to seize or freeze property that constitutes proceeds from crime or instrumentalities was mentioned by the authorities to represent the highest priority in judicial cooperation in criminal matters.

Table 52: GPO MLA – Seizure of Proceeds of Crime – Incoming Requests

Money Laundering Crime 2013-2018		
	№ of cases – received/ really executed (under Act 650/2005 Coll.)	**Total value of seized property (in brackets - procedure under Act 650/2005 Coll.)**
A movable thing	2/2 (2)	No quantified value
Real estate	5/4	EUR108 000
Money	16/7 (8)	EUR2 912 255 + USD1 649 (EUR2,542,282)
Securities	1/1	EUR365 134
Sum	24/14 (10)	EUR3 385 389+ USD1 649 (EUR2 542 282)
Other Predicate Offences (no request related to FT)		
A movable thing	22/14 (2)	EUR37 027 (EUR6 213) + other no quantified value
Real estate	1/1	0
Money	62/15 (5)	EUR3 050 793 + HUF 2 899 992 000
Securities		
Sum	85/30 (7)	EUR3 087 821+ HUF 2 899 992 000
TOTAL	109/44 (17)	EUR6 473 211 + USD1 649 (about EUR1 459) + HUF 2 899 992 000 (about EUR9 218 029)

623. The quantitative data can be seen in the table above, which also indicates how many of the requests has actually been executed and, in the right column, the values that have actually been recovered. The legal basis applied in executing the requests in most cases included the Strasbourg convention and, with EU member states, the certificate mechanism for the execution of orders freezing property pursuant to Council Framework Decision 2003/577/JHA as implemented by Act No. 650/2005 Coll. The AT were assured by the authorities that no such requests have ever been refused based on legal reasons, as the non-execution of requests was in most cases attributable to the absence of the expected proceeds on the respective bank accounts or otherwise in the territory of the SR, while other requests could not be executed because the same property had already been

seized in parallel domestic proceedings. Case examples show that in such circumstances, the foreign request would either be refused or, as a more favorable alternative, it would be recognized but, at the same time, its execution would be suspended with regard to the domestic measure (pursuant to Art. 12 of Act No. 650/2005 Coll.)

624. As regards the absence of assets to be seized, the authorities emphasized that in such cases the liquidation of the bank account had always taken place before the receipt of the foreign request and not during the time of its execution, which would normally take only a few days. In urgent cases, the cooperation with the FIU for suspending bank operations proved to be effective. According to the authorities, there is an increasing number of cases when the FIU is informed on the incoming request via its channels in advance and takes measures independently, while also informing the competent prosecutor thereof.

625. The total nominal value of assets seized upon foreign requests was around EUR15,3 million in the 5-years period although this is just an approximate figure considering that in most of the cases, the exact value of movable and immovable property items subject to seizure could not be determined. Case examples provided by the Slovakian authorities demonstrated their capability to successfully seize, on behalf of their foreign counterparts, various sorts of property beyond bank account money, including vehicles, real estate or company shares.

CASE BOX 16: Seizure based on a foreign freezing order

The competent prosecutorial authority from Hungary submitted a request for legal assistance to the District Prosecutor's Office Bratislava in January 2015, asking for the seizure of assets related to tax crimes committed in Hungary. The requesting authority attached a property decision (decision on ordering seizure of property) issued by the competent Hungarian LEA. The Slovakian prosecutor filed with the District Court Bratislava III a motion of order issuance pursuant to Article 551 (1) of the Code of Criminal Procedure, based on which the judge for pre-trial proceedings seized an amount of HUF 2 899 992 000 (about EUR10 000 000) on the bank account in the financial institution Slovenská sporiteľňa.

626. Requests related to ML offence represent a considerable proportion within the whole: 20% of the incoming and 25% of the executed requests are ML-related, which also goes for the volume of assets seized upon the ML-related requests (approximately EUR3 385 million throughout the entire assessed period). It needs to note that, for example, EUR108 000 worth of real estate and EUR365 000 of shares in commercial companies were seized upon 3 different ML-related foreign requests in 2016, including the one below. This, together with the steady increase in the number of ML-related foreign requests, may raise some doubts concerning the conclusions of the NRA according to which the SR is not a country attractive for placing proceeds from crime committed abroad.

CASE BOX 17: Seizure of business shares at the request of another state

The District Prosecutor's Office Trenčín was asked by the competent Czech prosecutor's office on 25 January 2016 for the recognition and execution of order of seizure of property – a business share of accused S. B. in the company with its registered office in the Slovak Republic. The order was issued in a criminal case being prosecuted in the Czech Republic for the criminal offence of money laundering. Based on the executed investigation, on 22 February 2016 the prosecutor of the District Prosecutor's Office issued the resolution recognising the order of the requesting State and prohibiting accused S. B. from disposing of her business share in the value of EUR365 134. The resolution was also sent to the District Court Trenčín for execution. The seizure of the business share has not been cancelled so far because the competent court in the Czech Republic has not issued a decision on the merits.

627. Assets seized in the SR on behalf of foreign requests may eventually be confiscated upon a foreign confiscation order submitted for recognition and execution, but as discussed above, no such action has ever taken place. Another option is to return the ill-gotten property to the victim of the predicate offence subject to criminal investigation in the other country, for which mechanism a case example was provided (see below). No other form of final decision regarding the seized assets was mentioned to the evaluators who neither received information on any practice in sharing of confiscated assets with other countries.

CASE BOX 18: Assets returned to the victims of the crime abroad

The District Prosecutor's Office Skalica supervised a criminal prosecution conducted for the offence of fraud, which consisted of phishing money from various victims in the Czech Republic. Based on the order of the prosecutor dated 4 September 2015, financial resources in the amount of EUR8 400 were seized on the Slovakian bank account of the suspect XY pursuant to Article 95 CCP.

After that, a motion was filed with the court pursuant to Article 95a CCP for returning a part of the seized money to one of the victims in the Czech Republic, which was granted by the court. Furthermore, communication was carried on with the Czech authorities which revealed, that a parallel criminal prosecution is conducted also in the Czech Republic for the criminal offence of fraud, in which two other victims (one Slovak and one Czech national) were registered. The Czech authorities requested legal assistance from Slovakia so that the rest of the seized money (EUR3 993) be returned to one of the victims in the Czech procedure. Eventually, the seized money was returned accordingly, and the criminal case itself was also handed over to the Czech Republic.

628. In the assessed period, Slovakian authorities successfully provided legal assistance to the Czech Republic regarding 4 requests in 3 separate cases related to terrorism-related and/or TF offences. In 2014-2015 assistance was provided in relation to a prepared terrorist act by means of special investigative means (undercover operation with interception) and in 2018 in relation to a similar offence, in which case several witnesses were heard and evidence was seized on behalf of the Czech authorities in 2 month time. In this case the perpetrator, who planned the terrorist attempt, was a Slovakian citizen residing in the Czech Republic, for which reason the Slovakian authorities also examined the domestic financial aspects of the act under preparation (but no TF offence could be detected). Finally, in 2018 two Czech requests were received and executed in relation to the Czech proceedings in the FT case parallelly investigated by the authorities of both countries as discussed more in details under IO.9 in which case the Slovak authorities performed a range of investigative acts on behalf of, and in close cooperation with the Czech authorities, also making use of EUROJUST assistance.

629. As regards how effectively the foreign requests for extradition are executed, the AT examined the two main regimes separately, that is, the traditional method based on international arrest warrants (IAWs) and extradition requests executed pursuant to the CCP and extradition treaties, and the one by which EAWs from EU Member States are executed under to the Law on EAW (Coll. 154/2010).

630. Since most of the incoming requests are dealt with in the EAW regime, there have not been too many traditional IAW-based extradition requests received and executed in the assessed period. As it can be seen in the table below (in which only the period 2014 to 2018 is covered) there have only been 30 such requests in these 5 years. Eventually, only approximately ¼ of these requests (8) were granted, while approximately ½ of the requests (16) were either refused (6) or the case was terminated otherwise (10). As for the requests executed, the AT were given some basic information regarding the timeliness of the proceedings (indicating a range from one to eighteen

months in general) which was however too general to draw any specific conclusions. On the other hand, half of these requests (4/8) were executed in a simplified procedure in which cases the timeliness was thus provided for.

631. Detailed description of the underlying cases proved that the majority of the refusals (5 out of 6) were related to foreign requests aimed at the extradition of Slovakian citizens, which is not allowed by the respective CCP provisions. While the Slovakian authorities expressed their willingness to initiate domestic prosecution in such cases upon the request of the respective foreign country and if the dual criminality standard is met, no exact information was provided regarding in how many of such cases the refusal to extradite was followed by such domestic criminal proceedings and with what results. On the other hand, at least one positive example was specifically mentioned by the Slovakian part. As a consequence, the effective applicability of the *"aut dedere aut iudicare"* principle in c.39.2 could not entirely be demonstrated.

632. As for the cases *"terminated otherwise"* these covered cases where the foreign request was either revoked or suffered from irreparable technical shortcomings – but also foreign requests which were not executed (hence refused) due to the lack of dual criminality. Unfortunately, the statistics were silent about the remaining 6 cases.

633. The countries most often submitting extradition requests were Serbia, the Russian Federation and the US. No significant ML/TF extradition cases were mentioned.

Table 53: Extradition from the Slovak Republic

	2014	2015	2016	2017	2018	Total
Extradition request received	5	7	10	1	7	30
Persons extradited (out of which: by simplified procedure)	2 (0)	1 (1)	4 (3)	0	1 (0)	8 (4)
Requests refused	3	2	1	0	0	6
Cases terminated otherwise	0	3	3	0	4	10

Table 54: Execution of EAWs by the Slovak Republic

	2014	2015	2016	2017	2018	Total
EAW received	171	161	182	169	167	850
Persons surrendered (simplified procedure)	98 (69)	84 (57)	122 (79)	110 (78)	111 (77)	525 (360)
Refused by courts	3	5	6	6	4	24
Cases terminated otherwise	70	72	54	53	52	301

634. EAWs are refused only exceptionally in application practice. Whereas 61% of the EAWs received from 2014 to 2018 (525/850) were reported to have been *"executed"* it is also clear that among the non-executed EAWs (39%) the refusals only represent a small portion and the rest of the cases were terminated for other, technical, reasons.

635. In the majority of the executed EAWs (360/525=68%) the decision was made in the simplified (prosecutorial) procedure, which further enhanced the timely execution of these requests (although the EAW procedures are generally regulated by strict deadlines as opposed to the IAW based procedure discussed above). The countries most frequently submitting EAWs were

the neighboring EU Member States (CZ, HU, AT) and among the incoming requests 1-3/year were related to ML.

636. As far as the non-executed EAWs are concerned, only a few of them were actually refused while the majority were *"terminated otherwise"*. This category includes cases where the requesting country has withdrawn the EAW (which covers most of such cases e.g. 30 out of 52 in 2018) as well as EAWs *"returned without decision"* (*e.g.* if the requesting country failed to provide supplementary information or when the surrender of a Slovakian national for the purpose of serving a sentence was substituted by a domestic recognition procedure). The few actual refusals were typically based on the absence of dual criminality (for the less serious *"non-catalogue offences"*) as well as cases of *res iudicata* or statute of limitations.

637. Within the prosecution service, 90 – 100 prosecutors work in this area out of which 13 prosecutors at the international department of the GPO (including the national member of the SR in EUROJUST who is currently the President of the EUROJUST), while the others at the level of regional prosecutor's offices (3-4/RPO in separate international units) and district prosecutor's offices (1-2/DPO who however may also additionally perform other duties too). The system is supplemented with a network of contact points of the European Judicial Network (EJN) (total 9 prosecutors with a central point at the GPO). These personnel resources appear sufficient and the same goes for the material equipment except the information system which was reported to be in need of improvement so as to provide a higher rate of added value also in terms of requirements for statistical data.

638. As for the MoJ, the Department of Judicial Cooperation in Criminal Matters has 10 staff which, considering the basically supportive role of the MoJ in an environment where most of the MLA cases are communicated through direct channels, should also be sufficient. No MLA-related specialisation can be found at the courts, but this was not reported to have caused any issues in providing or requesting MLA. Furthermore, a network of EJN contact points has also been established for the courts, consisting of minimum 2 senior court officials or judges at each court.

7.2.7. Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

639. Slovakian authorities claimed that requests for international judicial cooperation were submitted in all cases with foreign element. The Slovakian law does not contain conditions posing obstacles for effectively requesting evidence or detention of individuals with a view to their extradition. On the contrary, the prosecutor and LEA are considered to be legally obliged to obtain all evidence as required by Section 119 CCP and thus if there is any foreign element in a criminal case, it must at least theoretically be supported with evidence that is to be obtained by requesting legal assistance. Even if it might result in delays, there seem to be no mechanisms to avoid requesting assistance from abroad or the mechanisms available at LEA level are also based on maximizing the foreign evidence (see *e.g.* the requirement that whenever a transaction is postponed upon the suspicion that the assets are derived from crime and the bank sends a UTR to the FIU, the LEAs cannot proceed with investigating ML and seizing the frozen assets unless the FIU obtains from abroad and attaches to its dissemination a copy of the criminal complaint filed in the respective foreign country by the victim of the predicate offence (see below more in details).

640. As far as the duration of handling of requests for legal assistance is concerned, the Slovakian authorities recurrently complained that it takes much longer than the execution of foreign requests in the SR with the exception of requests addressed to the Czech Republic which are normally executed in 1-2 months. The total average handling time for requests (including EIOs)

in the assessed period was more than 6 months (187 days) which was just a little shorter for ML cases (an average of 140 days).

641. In reality, it means that for some overseas countries the execution of requests takes more than a year or several years while, on the other hand, requests sent in the form of an EIO to EU member states are usually executed in 2 months. The EIO was mentioned as a radical achievement not only in terms of timeliness and comprehensiveness, but also because the receipt and acceptance of an EIO is automatically confirmed by the recipient authority its timely execution can also be effectively demanded the Slovak judicial authorities have information whether and when the executing authority accepted EIO and they can effectively demand its execution. The involvement of EUROJUST in channeling EIOs was also reported to be very important in this respect. To avoid unnecessary delays or eventual non-executability of a request or EIO, the Slovak authorities tend to use such measures after obtaining preliminary information by LEA (including FIU) channels as to the feasibility of the request.

Table 55: Judicial Cooperation- GPO Outgoing Requests for Legal Assistance

	ALL total/direct legal contact	ML total/direct legal contact	FT total/direct legal contact
Submitted	**2013**		
	3 715/2 967	62/23	0
	2014		
	4 559/3 465	87/38	0
	2015		
	4 399/3 404	97/68	0
	2016		
	4 577/3 640	142/96	0
	2017		
	4 878/4 091	189/120	0
	2018		
	3 353/2 851	135/99	1
	Total		
	25 480/20 418	712/444	1

642. Approximately 80% of the requests were submitted using direct cooperation between prosecuting authorities while the same ratio is 62% for ML-related requests the number of which doubled by the end of the assessed period. This positive trend is attributable to the fact that most requests are addressed to the neighbouring and other EU member states by use of EU mechanisms based on direct cooperation.

Table 56: Prosecution Service – MLA requested

	2013		2014		2015		2016		2017		2018		Total	
	All	**ML**	**ALL**	**ML**	**ALL**	**ML**	**ALL**	**ML**	**ALL**	**ML**	**ALL**	**ML**	**ALL**	**ML**
AT	143	4/4	236	3/3	265		305	8/8	325	10/10	212	6/6	**1 486**	**31/31**
CZ	2 165	6/6	2 351	12/12	2 099	15/15	2 066	24/24	2152	19/19	1 746	23/23	**12 579**	**99/99**
FR	42	1/0	45	5/0	55	2/0	39	3/0	52	6/1	25	2/0	**258**	**19/1**
GE	167	10/1	260	11/2	306	21/21	277	24/23	314	28/28	168	14/14	**1 492**	**108/89**
NL				6/0			35			6/2			**35**	**12/2**
HU	388	11/11	417	20/20	466	22/22	521	30/30	491	47/47	207	23/23	**2 490**	**153/153**
PL	171		261	2/0	245	5/5	247	5/5	221	3/3	127	3/3	**1 272**	**18/16**
RO	63	1/1	57	2/0	57	1/0	85	3/0	110	4/4	48	5/1	**420**	**16/6**
UK	175	4/0	250	6/0	271	2/0	319		319	12/0	199	11/4	**1 533**	**35/4**
SUI	28		38	2/0	42	2/0	37		61	4/0	40	5/0	**246**	**13/0**

IT	67	9/1	102	5/0	73	5/0	77	8/3	109	10/3	32	9/4	**460**	**46/11**
USA	43		57	2/0	64	3/0	105		127	11/0	121	2/0	**517**	**18/0**
UA	33	4/0	48	1/0	36		24	3/0	47		44	2/0	**232**	**10/0**

643. The above table shows that the requests are sent mainly to the Czech Republic followed by other neighboring countries (in which context, unlike in terms of incoming requests, Ukraine is also represented) and Germany. It needs to note that the number of ML-related outgoing requests is generally higher than those received (especially in case of Hungary) which, however, is not true for the greatest recipient of Slovakian requests, the Czech Republic in case of which the proportion of ML-related requests is extremely low.

644. The vast majority of the requests referred to hearing of defendants or witnesses and production of documentary evidence including data subject to banking, tax or business secrecy while 10 % of the requests involved other legal assistance activities including search and seizure, the performance of special investigative measures etc. On the other hand, the GPO reported a recent increase in the number of requests for complex actions equal to a financial investigation (including BO information) particularly in USP cases. Slovakian authorities participate in the requested investigative acts abroad with regularity.

645. Areas in which evidence obtained from abroad proved to be essential are tax offences and cyber-criminality. As for tax crimes, a significant rise has been noted in terms of requests aimed at detection of fictitious deliveries of goods within the intra-Community trade related to VAT fraud schemes involving neighboring EU countries, by provision of documentary evidence, tax and accounting documents and interrogations. Similar attention is paid to cybercrimes such as phishing, copyright infringements and associated ML, in which relation content and operational computer data and banking data but also interrogation of witnesses (victims) was asked for. Awareness and attention in this field can be illustrated by the number of such requests (*e.g.* a total of 261 in 2018 as opposed to 65 requests of the same kind received in the same year.)

646. As far as requests for seizing property abroad are concerned, these were issued in rather limited numbers and involving moderate volume of assets throughout the assessed period. In ML-related cases, only one request was issued but without any effect. The low number might however be attributed to the fact that in practice, the FIU is usually asked for verifying the existence of bank accounts and actual balance (with a view to freezing the assets in the other country) before issuing a request for seizing money on bank accounts so that useless requests are not sent out.

Table 57: Judicial Cooperation GPO MLA - Seizure of Proceeds of Crime – Outgoing Requests

Money Laundering Crime 2013-2018		
	No of requests submitted/really executed (under Act 650/2005 Coll.)	**Total value of seized property (under Act 650/2005 Coll.)**
Money	1/0	
Sum	1/0	
Other Predicate Offences		
A movable thing	12/8	EUR136,002
Money	8/2	EUR402,167
Sum	**22/10**	**EUR538,169**

647. Movable things (indicated by amounts) would usually refer to the object of the criminal offence (cars, art objects etc.) or instrumentalities (mobile phones). Money was seized in moderate amounts apart from a single seizure of EUR330 000 in 2013. The predicate crimes were mostly offences against property.

648. Throughout the assessed period, there have been no property-related decisions (forfeiture/confiscation) submitted to the MoJ to be recognised and executed in other states, the reasons for which remained unexplained to the AT.

649. According to the GPO, no deficiencies in the format, contents or the legal basis of Slovakian letters rogatory or EIOs/EAWs have caused any delay or non-execution of the respective requests, particularly in case of the said EU instruments where the formal and content aspects are determined by the format to be used. As far as resources are concerned, reference is made to issues discussed above. In addition to that, however, the assessors learnt that the constant increase in expenses for translations poses a challenge for the prosecution service, as well as providing translators for non-European foreign languages.

7.2.8. Seeking other forms of international cooperation for AML/CFT purposes

650. FIU works with foreign counterpart authorities on the basis of non-contractual reciprocity, in accordance with the rules and standard conditions for exchange of information within the Egmont Group, also respecting the relevant national law of the respective foreign FIU. However, according to the requirements of partner authorities that need a signed MoU for their effective international cooperation, the FIU is ready to sign a MoUs with them so as to ensure the legal basis for information exchange, as it happened in 8 cases (see in the TCA).

651. International cooperation between FIUs is not limited to specific cases of information exchange but it also involves the general exchange of experience, best practices and engagement in the international working groups and organizations. Activities of the FIU in international cooperation are carried out in accordance with the methodological guidance of the FIU Director issued by FIU in 2018 that contains all detailed instructions, methods, operations on the content and formal requirements for handling all agenda of the department of international cooperation of FIU.

652. The FIU seeks for assistance from abroad through its department for international cooperation by sending its own requests to the partner FIUs (in relation to verification of UTRs or reports of cross-border transportation of cash received from the Customs authorities), as well as requests on behalf of other departments of the Police Force (in relation to verification or investigation of suspected ML/FT).

653. FIU sends its own requests through INTERPOL in very limited cases when a foreign FIU cannot provide information, due to legal reasons, without a signed reciprocal MoU (reference was made to a non-EU country overseas) or if the foreign FIU does not meet the standard requirements for exchange of information yet and thus it has not been connected to the ESW network discussed below. The FIU also receives spontaneous information from foreign partner FIUs which is then verified and either saved in its internal database or passed on to the relevant competent state body for intelligence purposes.

Table 58 : FIU international information requests

	2013	**2014**	**2015**	**2016**	**2017**	**2018**
Requests sent by the FIU	250	333	166	78	89	**85**
Spontaneous sharing of information received by the FIU	**78**	**70**	**126**	**156**	**211**	**420**

654. According to the authorities, the decrease in the number of requests sent to foreign FIUs can be attributed to the improvement of the cooperation between the FIU and Slovakian banks. In

the first part of the assessed period, the banks submitting a UTR did not provide FIU with all information the competent LEAs would require in order to deal with postponed transactions. For example, as noted above, LEAs need a copy of a criminal complaint filed in the respective foreign country by the aggrieved subject so that they can proceed with the domestic ML case and with seizing the assets. In such cases, the FIU had to request such information and data from foreign counterparts but, as a result of efficient negotiations between FIU and banks, the latter have adapted their policies and, in case of postponement of a transactions, they immediately ask the correspondent bank for providing the required data (*e.g.* the aforementioned criminal complaint) so that the FIU need not send out a request for this purpose.

655. Exchange of information between FIUs within the membership in Egmont Group is carried out through the secure and encrypted Egmont Secure Web (ESW). In addition to that, the Financial Intelligence Unit Network (FIU.NET) is also available between FIUs in EU member states enabling FIUs connected to FIU.NET to compare their data with those of other FIUs without the use of sensitive personal data so as to identify various links to crimes in other countries.

656. According to illustrative data from the year 2017, the countries to which FIU sent their requests for information through the ESW communication network were mainly the United States (6), Russia (3), Switzerland (2) and Turkey (2) while requests through the secure FIU.NET network were sent primarily to the Czech Republic, Hungary, Germany and the Netherlands. Foreign FIUs mostly respond to the requests duly and within reasonable time (from several days to several weeks).

657. The requests mostly concerned information about foreign bank accounts (holder or authorized users, ultimate BO in case the holder is a legal entity) verification of authenticity of documents presented to a Slovak bank when opening an account or making bank transactions, criminal records and record in internal FIU databases, information on the criminal proceedings initiated in the other country etc. In addition to that, the FIU may ask also for the postponement of a suspicious transaction on a foreign bank account or adoption of measures aimed at postponement of eventual debit transactions. In such cases (1-2 of which occur every year) once the postponement is successful, FIU Slovakia would surrender the case to the competent Slovak LEA so as to prepare an official request for further legal assistance for the purpose of prosecution and seizing the funds.

658. The Office of International Police cooperation of the Police Force Presidium (UMPS) is the central point for exchange of information in the framework of international police cooperation for all offences falling within the scope of competence of the office including the predicate offences acting as an intermediary for exchange of operational, strategic and other information between the competent departments of the Police Force, other relevant Slovak authorities and the foreign partners. The UMPS includes the EUROPOL and INTERPOL National Units too and provides for exchange of information through these channels, both on a 24/7 basis. The EUROPOL National Unit ensures international police cooperation with EU member states and third parties through the secure SIENA channel (Secure Information Exchange Network Application).

659. To the extent the EUROPOL database is searchable for these purposes, the Slovakian authorities provided the following figures on Slovakia-related SIENA documents with identified ML offence, which demonstrate the relevance and the added value of Europol contribution (ARO related data specifically for ML communication were not available and thus are not included).

Table 59: SIENA ML Communication (without ARO)

Year	Received	Sent
2013	6	2
2014	81	20
2015	48	18
2016	141	61
2017	589	305
2018	692	352

660. Among other means of exchange of information that have reportedly been used by Slovakian LEA with regularity are the Schengen Information System and other tools of Schengen police cooperation (SIRENE channel) are used for monitoring movement of persons, documents, vehicles and objects. CTU - NAKA is connected via PWGT (Police Working Group on Terrorism) channel with counter-terrorism units of all EU countries + Switzerland and Norway, enabling immediate exchange of information concerning detection, investigation, clear-up and documenting of terrorist crimes.

661. Cooperation through police attachés accredited in Slovakia and through the police attachés of the Slovak Republic accredited in other states was also mentioned as a helpful instrument. Currently, there are 16 Slovakian police attachés posted abroad, located in and/or accredited for all neighboring countries as well as other relevant EU and non-EU jurisdictions[52] also assisted by 2 liaison officers at the Slovakian Liaison Bureau of the EUROPOL, all directly involved in general and operational bilateral Police cooperation with counterparts in the respective countries (the same way as foreign police attachés are authorized to directly contact Police bodies in Slovakia.) In addition, this mission is organized and managed by the UMPS with a view to enhance their integration within the international police cooperation.

662. Non-confidential requests for international police cooperation delivered to the office are usually recorded in the International Police Cooperation Information System which is the case management system used especially by UMPS Central Bureaus. This system helps to avoid the duplicated handling of the same requests through several bureaus/channels for cooperation. The sensitive files can be locked which reduces the number of persons having access to the file and its documents while every step and work step in the file (logs) are recorded in detail. Priority requests are handled immediately or preferentially within the deadlines specified by the requesting party.

663. The ARO - NAKA exchanges information and cooperates with third countries also in the framework of the Camden Assets Recovery Inter-Agency Network (CARIN) using encrypted SIENA communication channels. The ARO receives and handles the requests of ARO/CARIN Offices of other countries for tracking and identifying criminal proceeds that may be the subject of freezing, seizing or confiscation. The ARO submits such requests on behalf of domestic LEA with a moderate frequency (5 cases in 2013, 4 cases in 2014 and 2015 respectively and 5 in 2018, one of which is described in the case box below). The countries to which the requests are submitted most frequently and countries submitting most requests are the Czech Republic, Hungary, the United Kingdom, Poland, Austria and Germany.

CASE BOX 19: ARO international cooperation in drug case "SKALKA"

In the context of the criminal proceedings against the accused P.Č. and others for exceptionally serious

[52] AT/SLO, BG, CRO, CZ, DE, HU, IT, MNE/AL, PL, RO/MD, RU, SR/NMAC, UA, UK and US

offence of unauthorised production, handling and trafficking of narcotics etc. (Art. 172 CC) and other offences, investigated by NAKA, the investigator handled and submitted through ARO Slovakia a request for identification of property of three of the defendants in other states so as to secure those assets for the purposes of the punishment of forfeiture of assets. Consequently, ARO successfully identified, through the members of international network of agencies dealing with cross-border identification, freezing, seizing and confiscation of proceeds of crime, various assets of the defendants in the territory of Czech Republic, Poland and Germany where, according to the findings, the criminal contacts and activities of the defendants had extended.

664. Neither the FIU nor LEAs reported to have any legal or operational issues affecting their cooperation with the foreign counterpart authorities. Problems arisen in this area were more of a general nature such as the limitations imposed by foreign FIUs regarding the further use of information they provide (and thus disabling the use of that information by e.g. by LEAs). As far as adequate resources for international cooperation are concerned, the FIU expressed that human resources particularly at the department of international cooperation are insufficient (with only four employees and the Head of Department) but it has not yet had an impact on the timeliness and accuracy of the assistance provided. No issues of resource were reported by other authorities.

665. Indirect exchange of information by FIU and LEAs with foreign non-counterpart authorities only takes place with a limited regularity. In case a foreign FIU makes such a request, the Slovakian FIU would provide information even for a third party (a partner of foreign FIU in the other country) which mainly occurs in case of requests made on behalf of LEAs of the respective foreign country. Most of such requests come from neighboring EU member states (CZ, HU) in which cases the FIU would provide the requested information to the requesting foreign FIU but with a handling code/consent so as to authorize the foreign FIU to disseminate information to their competent LEAs. As for Police bodies, such cooperation is only possible between members of police forces and in case of non-confidential information *e.g.* for faster execution of requests. No indirect exchange of information for banking sector is carried out in Slovakia.

7.2.9. Providing other forms international cooperation for AML/CFT purposes

666. FIU processes requests from foreign FIUs for provision of information without undue delay and sends it through the channels mentioned above provided that the foreign request meets the minimum criteria as defined by the Egmont Group principles for exchange of information (link to the country to which the request is directed, sufficient reasons for ML/FT suspicion, exhaustive description of the case). If the request does not meet these minimum requirements, the FIU is not obliged to process it, but even in such cases the FIU would usually provide at least information from its own internal databases. If the request goes beyond the competences and scope of activity of the Slovakian FIU (e.g. when it concerns identification of a person or obtaining documents kept by another state body) the respective part of the request is passed on to the competent authority while notifying the requesting foreign FIU.

Table 60: Information requests received and sent by the FIU

	2013	2014	2015	2016	2017	2018
Foreign requests received/executed by the FIU (none refused)	258	301	288	321	265	**240**
Spontaneous sharing of information sent by the FIU	**293**	**430**	**390**	**321**	**654**	**555**

667. No foreign requests for information were refused by the FIU in the assessed period (in some cases, however, as mentioned above, the assistance was limited to information from FIU internal databases). Urgent requests were answered in a period from several hours up to 2 days according to the volume of the requested information, while standard requests within a time limit under FIU.NET rules or within 30 days or in a longer time. Periods longer than 30 days occurred only exceptionally and resulted from external reasons such as failure of financial institutions or state bodies requested to provide information in due time. The foreign requests mostly concerned information in same scope as outgoing requests discussed above.

668. The information exchanged may only be used by the counterpart FIU for analytical/intelligence purposes. Information can be further passed on to LEAs for intelligence purposes with the explicit consent of the Slovakian FIU which, however, is granted automatically in all cases by a disclaimer included in the document serving for provision of information. Foreign counterparts are also notified that if the information needs to be used as evidence in criminal proceedings, it is necessary to request it through MLA.

669. The FIU provided information to its foreign counterparts without a prior request (spontaneous information) meeting at least the minimum criteria in terms of content and extent, with a remarkable regularity. In such cases, the FIU would usually try to provide as much information that is available.

670. The FIU receives and executes intermediated requests for information concerning verification or investigation of ML/TF cases from foreign Police authorities via INTERPOL or EUROPOL. Illustrative data from 2017 show that the countries the most frequently requesting information from FIU through the ESW communication network were Germany (7), Austria (6), the United States (5), Italy (5) and Russia (5) while through the FIU.NET Hungary, the Czech Republic, France, Poland and Italy.

671. The FIU has received several urgent requests for freezing / seizing of funds on Slovakian bank accounts (16 in 2016 and 6 both in 2017 and 2018). In such cases, the FIU informed the counterpart authority that FIU Slovakia is not authorized to freeze such funds but to postpone unusual transactions (Art. 16 AML/CFT Act) which can be applied also upon request of a partner FIU. In such cases the FIU contacted the banks immediately, asking for information on the respective bank account and, if the money was still on the account, for the postponement of the transaction or adoption of measures aimed at preventing possible debit transactions. However, in most cases the funds were no longer available on the account (in which case the FIU obtained information from the bank on the further financial flow for the information of the foreign partner) or the request arrived before the respective transaction had been accredited to the Slovakian bank account (in which case the incoming money was then immediately returned by the bank itself).

672. The ARO receives requests from its foreign counterparts with regularity (2013 - 48, 2014 - 78, 2015 - 61, 2016 - 81, 2017 – 91 and 2018 - 103). If the request of the partner office for tracing and identification of proceeds is not completed in compliance with the respective EU legislation (Council Framework Decision 2006/960/JHA) and does not contain the necessary particulars, it cannot be executed until the requesting country provides supplementary information. The ARO was unable to specify how many of the requests needed additional information and how many were eventually refused.

673. The NBS was reported to have successfully cooperated with foreign supervisory authorities in executing incoming AML related requests (while no such domestic requests were submitted in the same period). The requests of such counterpart authorities extended to confidential data about

clients, bank accounts and transactions. The NBS has executed all but one incoming requests by submitting the information as *"released from professional secrecy"* in a timely manner, respecting the 60 days deadline for response prescribed in the applicable law. The exception was a request submitted by the Central Bank of a non-EU jurisdiction in 2018 in which respect the NBS was not able to provide information in accordance with the respective EU legislation. All other requests in the table below were submitted by counterpart authorities from EU member states. In other sectors (insurance, securities, OFI) no request for international cooperation by foreign supervisory authorities was recorded.

Table 61: International cooperation by the NBS

	2013		2014		2015		2016		2017		2018	
	ML	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	FT
Foreign requests received by supervisory authorities related to ML/TF	0	0	1	0	0	0	0	0	4	0	7	**0**
Foreign requests executed	0	0	1	0	0	0	0	0	4	0	6	**0**
Average time of execution (days)	**0**	**0**	**60**	**0**	**0**	**0**	**0**	**0**	**40**	**0**	**40**	**0**

7.2.10. International exchange of basic and beneficial ownership information of legal persons and arrangements

674. The relevant analysis can be found in relation to Core Issues 2.3 and 2.4 above, in relation to which the following can be added here.

675. As regards judicial cooperation, providing information about the BOs of LPs for foreign judicial authorities is carried out within the regime described above and in the same scope as in the case of national proceedings. The content of information of the Business Register, Trade Register, Register of Partners of Public Sector and Register of Legal Entities, Entrepreneurs and Public Authorities kept by the Statistical Office of the Slovak Republic but also of other registers (Register of Non-Investment Funds, Register of Non-Profit Organizations providing Services of General Economic Interest, Register of Foundations) is standardly sent to the foreign judicial authorities. There are no obstacles for applying such procedure within the framework of judicial cooperation in the criminal matters. If the matter is identified as urgent or automatically in linked cases the request can be handled even in a couple of days. BO data are typically requested by foreign counterpart authorities as part of other, associated evidence relevant in this field (including banking documents, witness interviews etc.).

676. In case data of legal persons are requested within FIU-FIU communication, FIU Slovakia applies, beyond the databases and systems mentioned above, its own information system NetReveal, intermediated and updated information from the FDSR on registered entrepreneurial bank accounts of legal persons, on arrears of taxes and on excess VAT deductions, information from the Register of Persons of Police Interest on persons in whom the police is interested - partners and executive directors of legal entities as well as the information systems of the MoI (criminal information/records of partners and executive directors of legal entities in the police databases DVS[53] and CLK[54], identification data of partners and executive directors of legal entities

[53] DVS–The Register of Investigation Cases and Criminal Records

in the police databases REGOB[55], ECU[56], information from The Trade Register and the research information system of the FDSR on taxable entities (containing a detailed overview of information about the business entity in respect of taxes, types of taxes, bank accounts, property relationships, paid excess deductions, results of previous inspections, economic result and balance of assets and liabilities, etc.). All request of foreign FIU for basic information on legal person and the UBO have been handled positively so far.

Overall conclusions on IO.2

677. Slovakia provides to a large extent constructive and timely MLA using the EU legal instruments, bilateral and multilateral agreements. The majority of incoming requests received are from EU Member States. The number of foreign requests refused or not executed is very low. Such refusals happen due to objective technical reasons or failure of the requesting authority to provide additional information. Only in rare cases the dual criminality standard has been an obstacle in providing legal assistance. LEA and the FIU are actively seeking and providing other forms of international cooperation in an appropriate and timely manner without any undue delay with their foreign counterparts. The LEAs provide information on the BO to foreign counterparts in the course of criminal proceedings without obstacles. The FIU provides all relevant and available data on basic information and the BO of legal persons using its own databases and information that can be obtained from other sources.

678. **Slovakia is rated as having a Substantial level of effectiveness for IO.2.**

---

[54] CLK–The Central Register of Subjects (identification of person and possessions of persons/subjects)

[55] REGOB - The Slovak Population Register

[56] ECU - The Register of Foreigners

TECHNICAL COMPLIANCE ANNEX

This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in numerical order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2011. This report is available from https://rm.coe.int/report-on-fourth-assessment-visit-anti-money-laundering-and-combating-/1680715cbc.

Recommendation 1 – Assessing risks and applying a risk-based approach

This is a new Recommendation that was not assessed in the 2011 MER.

Criterion 1.1 – The legal obligation for FIU to conduct the NRA is provided by Art. 26(a) of the AML/CFT Act and by Art. 7 of the Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The obliged persons, the NBS, law enforcement authorities, other state authorities and institutions shall participate in preparing and updating the NRA and shall be obliged to provide the necessary assistance to the FIU. The risk assessment takes into account the risk assessments conducted by the EU and other international institutions. The first round of the NRA was conducted for a period of 2011 – 2015, based on a decision of MISO-LP (since February 27, 2018, the group has been renamed to NES LP). The NRA process started in November 2016 and the final workshop on NRA with the participation of the World Bank took place in November 2017. In summer 2018, the elaboration of non-public and public report from NRA was completed (the public was made available on the FIU website).

Criterion 1.2 – The responsible authority for the preparation and updating of NRA is FIU. According to Art. 26 (a) of the AML Act, the FIU is also the only coordinator of NRA (other participants shall participate in preparing and updating the NRA based on FIU demand). NES-LP is a subsidiary mechanism (instrument) for the preparation of the NRA.

Criterion 1.3 – Art 26 (a) (3) of the AML/CFT Act provides that NRA shall be updated, in particular when there are developments in the ML/TF risks, and depending on the activity of EU bodies. There are no timelines for the NRA up-dates. Nevertheless, this shortcoming is partly addressed by the AP which tasks the MoI (in cooperation with the MoF, the MoJ, the General Prosecutor, the Governor of the NBS and the Director of the SIS) to update the NRA. No up-date was done at the time of the on-site visit.

Criterion 1.4 – The main mechanism used to provide information on the results of the NRA was through publication on the FIU website and through conferencing/trainings. To disseminate the results of the NRA to prosecutors a document was prepared by the GPO. Although mechanisms are in place, since there is no legal obligation to provide information about the results of the NRA to all relevant competent authorities, self-regulatory bodies and RE, the criterion is not fully met.

Criterion 1.5 – At the MoI level, the AML/CFT AP provides the increase in the scope and quality of analytical capacities in the area of AML/CFT. An increase in the personnel capacities of the FIU and of NAKA to enhance the number of controls of obliged entities is also foreseen. Same goes for the NBS positions dedicated to supervise financial institutions. Apart from allocation of resources, are no references to the risk based preventive and mitigating measures.

Criterion 1.6 – The SR has not taken any decision not to apply the FATF recommendations, except for the CDD exceptions for simplified DD within the meaning of Articles 11 and 11a of the AML Act.

a) Article 11(1) and (2) of the AML/CFT Act provides for the possibility of applying simplified CDD measures in certain scenarios (limited financial services and low thresholds), which are not justified by the findings of the NRA. The authorities did not provide any other relevant analysis of risks that underpins those scenarios. Nevertheless, the legal provisions do include some mitigation measures as it applies only to: i) electronic money which cannot be deposited repeatedly, and the maximum amount will not exceed EUR 250 or EUR 500 for use only on the territory of SR and ii) payment services provided through the public electronic communication network provided that the value of one transaction does not exceed EUR 30 and at the same time, the total monthly limit of payments made from one telephone number does not exceed EUR 250. The payment devices can be used exclusively for purchases of goods and services and they cannot be funded by anonymous electronic money.

b) The exemptions do not concern a financial activity carried out on a very limited or occasional basis.

Criterion 1.7 – According to Art. 20a of the AML/CFT Act, the obliged person shall be obliged to identify, assess, evaluate and update the ML/TF risks according to the types of transactions and business relationships, taking into account its own risk factors and the risk factors listed in Annex No. 2 of the Law.

a) According to Art. 10 (4), the obliged persons shall determine the scope of CDD measures in respect of the ML/TF risks. In assessing the ML/TF risks, the REs shall be obliged to evaluate and consider the risk factors listed in risk assessment pursuant to Art 20a (1) of the AML/CFT Act.

b) Art. 20a (2) of the AML/CFT Act provides that the REs risk assessments must be adequate to the nature and size of the obliged person and must consider the results of the NRA.

Criterion 1.8 – According to Art. 11 of the AML/CFT Act, financial institutions, as well as DFNBPs, may only perform simplified due diligence (SDD) for a customer representing a low risk of ML/TF according to their specific risk assessments (see also c.1.7(b)). Nevertheless, the deficiency identified under c.1.3 impact on the rating of c.1.8.

Criterion 1.9 – Pursuant to article 1(3) (a) of Act on financial market supervision 747/2004, and article 11 (1) of the Act on Gambling Games 171/2005, specific supervisory authorities are required to supervise compliance by RE, including compliance with AML/CFT requirements and to determine whether the measures taken by the entities to limit the risks posed by their operations are sufficient. The AML/CFT risk assessment is regulated in Art. 10(4), Art. 20, Art. 20(a), Art. 26(a) and Art. 29 of the AML/CFT Act.

Criterion 1.10 – Pursuant to article 20a (1) of the AML Act, the obliged person shall be obliged to identify, assess, evaluate and update the ML/TF risks according to the types of transactions and business relationships, taking into account its own risk factors and the risk factors listed in Annex No. 2 of the Law. Following Art. 20(1) the obliged person shall work out and update the programme of its AML/CFT activity so that its contents and focus allow to fulfil duties according to the AML Act.

a) Art. 20 (1) of the AML/CFT obliges the REs to prepare a written and up-dated document aimed at the prevention of ML/TF: the “Programme”. The Programme should contain primary elements, among which the ways to assess and manage risks as referred to in Art. 20(2)(c) AML/CFT Act.

b) REs shall determine the risk factors according to: the type of product, the value and manner of conducting the transaction and the risk of the country or geographical area to which the business relationship or transaction relates (Art. 20(a)(1) of AML/CFT Act). The risk assessment must contain the specification of the methods and types of measures by which the obliged entity manages and mitigates risks in its activities, carries out internal control and checks personnel. The risk assessment shall be proportionate to the nature and size of the obliged entity and shall take into account the results of the NRA (Art. 20(a)(2) of AML/CFT Act). The AT is of the opinion that this list contains all the relevant risk factors.

c) The obliged person shall be obliged to update the Programme. In particular up-dates shall be carried out when there is a change in the activity of the obliged person or before starting to provide new products if the change can affect the ML/TF risk (Art. 20(1) of AML/CFT Act);

d) There are no defined mechanisms for providing risk assessment information to competent authorities and SRBs.

Criterion 1.11 – a) Art. 20 (1) of the AML/CFT Act require all REs to have internal AML/CFT Programs as described under 1.10. Pursuant to Article 20 (2) (c) the RE's AML/CFT programs shall contain risk assessment and management including by taking into account the results of the NRA. The AML/CFT program shall be approved by the statutory body of the obliged person which amounts to "senior management".

b) Art. 20 (2) (k) of the AML/CFT Act stipulates that the Programme shall contain a description of how the obliged person controls (monitors) the implementation of the AML/CFT activities.

c) There are no provisions to oblige the REs to take enhanced measures to manage and mitigate risks where higher risks are identified, beyond EDD measures.

Criterion 1.12 – The only simplified measures allowed by the AML/CFT Act pertain to CDD. The simplified CDD measures can be taken when the clients have a low risk of ML or TF. The application of simplified measures is not permitted in the case of an ML/FT suspicion. Nevertheless, the shortcoming under c 1.10 and 1.11 impact the rating.

Weighting and Conclusion

There is no legal obligation to provide information about the results of the NRA to all relevant competent authorities, self-regulatory bodies and RE. The assessors were not provided with any piece of legislation or Action plan demonstrating a RBA in allocation of resources and implementing measures to prevent and mitigate ML/TF. There are no provisions to oblige the REs to take enhanced measures to manage and mitigate risks where higher risks are identified, beyond EDD measures. **Recommendation (R) 1 is rated partially compliant (PC)**.

Recommendation 2 - National Cooperation and Coordination

In the 3rd evaluation round, former R. 31 was rated PC. In the 4th MER (2011), the rating was also PC, based on the lack of sufficient coordination between significant players of the AML/CFT regime, the need for more effective mechanisms to co-ordinate at the operational level, the need for more detailed statistics across the board to assist properly coordinated policy analyses (former R.32, see R.33 on statistics), and the lack of effective use of the mechanisms in place.

Criterion 2.1 – In 2011, the Strategic Plan for Combating Money Laundering and Terrorist Financing for 2012 to 2016 was adopted by the Government, which was based on then-known methods of ML and TF. The Strategic Plan contained forecasts and recommendations to be put in practice by the FIU (as the central coordinating body for AML/CFT issues). The National Expert

Group on Counter-Terrorist Financing (NES-FT) has adopted the National Action Plan to Combat Terrorism for 2015-2018 (CT-NAP). CT-NAP is a strategic document, which must be endorsed by the Slovak Government. In August 2019, the new CT-NAP for 2019 – 2022 as well as the Evaluation report of CT-NAP for 2015 – 2018 were under approval with expected adoption by the Slovak Government in October 2019.

Following the adoption of the NRA in 2018, new Strategic Principles to Combat Money Laundering and Terrorist Financing for 2019 to 2024 and an Action Plan to Combat Money Laundering and Terrorist Financing (AP) for 2019-2022 in the process of being implemented by individual ministers have been prepared.

A number of other guiding documents and action plans were adopted on topics which relate to ML and TF, such as the Action Plan on Migration Policy (2018-2020), the Strategy on Prevention of Crime and Other Anti-Social Activities (2016-2020), the National Programme and Action Plan for Combating Trafficking in Human Beings (2019-2023) and the National Integrated Border Management Strategy (2019-2022) Action Plan Against Tax Frauds (2017 – 2018).

Criterion 2.2 – The Interdepartmental Expert Coordination Body on Combating Crime (MEKO) is the national body for strategic coordination of combatting crime between relevant authorities. MEKO coordinates and enables the information exchange between domestic bodies to develop and coordinate activities on combatting crime. It also initiates legislative proposal to improve interdepartmental cooperation on combatting crime. AML/CFT policies and activities are thus one of many areas which MEKO coordinates. On this platform tasks are adopted, and the respective authorities are responsible for their implementation. Representatives of the MoI, MoF, MoJ, Minister of Transport and Construction, the GPO, Military Intelligence and the SIS are members of MEKO. Within MEKO, 14 expert groups (including NES-LP, see c.2.1), subdivided into 15 subgroups, function to develop and coordinate policies on combatting crime. NES-LP is responsible for national AML/CFT policies within the scope of MEKO's mandate. By August 1, 2019, 470 members from 75 institutions were registered.

Criterion 2.3 – The mechanism enabling the policy makers and the relevant authorities to develop and implement the AML/CFT policies and activates is a combination of MEKO and the National Expert Group on Anti-Money Laundering (NES-LP).

NES-LP is headed by the Director of FIU Slovakia and includes NBS, the MoF (the authorities for AML/CFT control/supervision) and other relevant bodies[57]. Most of the institutions contributing to NES-LP are considered to be policy makers in the area of AML/CFT The purpose of NES-LP is to enhance ways of exchanging operational ML/TF information within the framework of the current legislation, and to coordinate activities related to detecting and talking organised crime.

Other subgroups and working groups may be and have been created to counter crime and enhance cooperation and coordination (e.g. MEKO's expert group on human trafficking, MEKO's interdepartmental expert working group to combat corruption). Within the NAKA, a number of working groups have been set up focused on eliminating ML, TF and terrorism (e.g. interdepartmental working group of development of legislation in the area of freezing of funds).

[57] The Presidium of the Police (Anti-Corruption, Anti-Drug, Financial, Counter-Terrorism and Criminal Counter), the Police College in Bratislava, Criminal Office of the Financial Administration, General Prosecutor's Office of the Slovak Republic, Ministry of Justice of the Slovak Republic, Slovak Information Service, Military Intelligence, Ministry of Economy of the Slovak Republic, Ministry of Foreign and European Affairs

Criterion 2.4 **–** In 2017, a subgroup within NES-LP was established to combat TF and PF (Resolution of the Coordination Body No. 7, 14 February 2017), which has gathered once in 2017. Meetings may be attended by the members of NES-LP, as well as other relevant competent authorities and supervisors, such as the Slovak Banking Association, the MoJ and the Criminal Police Office on environmental crime. The sub-group is responsible for analysing the state of TF and PF, for developing rules on information exchange among the members, and for identifying shortcomings in the mechanisms to combatting TF and PF mechanism.

Criterion 2.5 **–** The FIU, NBS, MoF are empowered and obliged to co-operate with the Office of Personal Data Protections (OPDP) which is the state authority competent to supervise the respect of personal data protection regulations.

The FIU cooperates with the OPDP through the Personal Data Protection Department of the Inspection Service of the MoI. An example of such a cooperation are the consultations on how the documents should be processed in the FIU information system, in compliance with the EU Regulations 2016/679 and Act 18/2018 on personal data protection.

The NBS continuously consults OPDP on current issues arising from activities related to financial market supervision. The OPDP directly contacts the NBS in order to jointly resolve any identified deficiencies. Alternatively, the OPDP may directly contact the bank in order to jointly resolve any possible deficiencies. In practice no such deficiencies have been identified in the AML/CFT area.

Weighing and Conclusion

All the criteria are met. **R.2 is rated Compliant (C).**

Recommendation 3 - Money laundering offence

FATF Recommendation 3 of 2012 and its interpretative note merges and somewhat restructures the previous Recommendation 1 and Recommendation 2. The latter was rated C in the 2011 MER. Recommendation 1, however, attracted a rating of PC. In addition to concerns regarding effectiveness, a matter addressed elsewhere in this evaluation, two identified deficiencies contributed to this ruling. First, the definition of 'property' was not sufficiently clear and the ML offence did not clearly extend to the indirect proceeds of crime. Second, not all designated categories of offences were fully covered as predicates as there was no full criminalisation of the financing of an individual terrorist's day to day activities or of the financing of the acts defined in the treaties annexed to the UN TF Convention. In so far as the first of the deficiencies is concerned the SR has amended both Section 130 and Section 233 of the CC; both are considered further below. As detailed in the discussion of technical compliance with R5, the SR has also sought to address the deficiencies flowing from its earlier approach to the terrorist financing offence. There are few new FATF requirements in this context when compared to the methodology applicable to the 2011 mutual evaluation.

Criterion 3.1 **–** The SR is a party to both the 1988 UN Vienna Convention and the UN Palermo Convention of 2000. The ML is criminalised through Section 233 CC ("Legalisation of income from criminal activity" in the original, but translated and referred to as Money Laundering) which refers to laundering the proceeds of a crime committed by any person, which covers self-laundering. The "legalisation" is defined as disposing of a thing when motivated by an effort to conceal such income or thing, disguise their criminal origin, conceal their intended or actual use for committing a criminal offence, frustrate their seizure for the purposes of criminal proceedings or forfeiture or confiscation. Income or other property obtained by crime is covered.

The broad language used in Section 233 comprises the elements listed in Article 3(1)(b) & (c) and Article 6(1) of the Vienna and Palermo Conventions respectively (see para 45, 46, 47 of the 4th round MER) but with some notable exceptions as far as the purposive element is concerned.

Pursuant to Section 233 any form of the ML offence can only be committed with the intention (i) to conceal the existence of the income or items (which have been derived from criminal activity) or (ii) to conceal their origins in the criminal activity, or their determination or use for the commission of a criminal offence, or (iii) to obstruct their seizure for the purpose of criminal proceedings or their forfeiture or confiscation. Proving a purposive element is thus required not only for the conversion and transfer type ML activities but to all other forms too, including the acquisition-possession type activities in Section 233(1)(b) which are not considered ML unless committed with a concealment or obstruction purpose. In addition, the ML offence does not cover the conversion or transfer of property for the purpose of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his/her action, as this purposive element is missing from Section 233 CC.

This gap is to some extent mitigated by the offence of *"sharing"* in Section 231 CC which is a more traditional but less serious, receiving-type offence that criminalises, without requiring any purpose on the mental side, the use and handling of items derived from a criminal offence. The scope of *"sharing"* is, however, significantly narrower than the ML offence and it only applies to persons other than the perpetrator of the predicate offence. As a result, any ML acts committed by the offender with knowledge of the criminal source but without a demonstrable intent to conceal would be covered by neither Section 233 nor Section 231 and are therefore not criminalised.

Criterion 3.2 – The 2011 MER concluded that the SR had, in effect, adopted an 'all crimes' approach to the issue of predicate offences for ML (para.52). The soundness of this view has been reinforced by amendments to Section 233(1) of the CC which, *inter alia*, replaces the term *'criminal offence'* with the broader concept of 'criminal activity' (Act 397/2015). The financing of terrorism constitutes a predicate offence for money laundering.

Criterion 3.3 – The SR does not apply a threshold approach or a combined approach that includes a threshold approach. Consequently, this criterion is not applicable.

Criterion 3.4 – As noted above, the 2011 MER concluded that the definition of 'property' was not sufficiently clear and that the ML offence did not clearly extend to the indirect proceeds of crime. For reasons intimately connected to the structure and traditions of the Slovak legal system as a whole it was determined that the most appropriate way in which to respond to the findings and recommended action in the 2011 MER would be by revisiting the definition of *'thing'* (aka*'item'*) in Section 130 of the CC. This was taken forward by Act No. 397/2015 which entered into force on 1 January 2016. As noted in *'Complementary information on legislative measures concerning the compliance with the Recommendation 3'*, submitted to the Moneyval Secretariat in August 2019, 'the intention was to be fully in line with the requirements of MONEYVAL'.

The amendment in question added four elements to Section 130(i) namely, (d) funds on an account; (e) proceeds from a criminal activity as well as the profit, interest and other benefits arisen (sic.) from such proceeds; (f) a document that forms a basis for exercising a legal entitlement; or (g) a proprietary right or other value appreciable (sic.) in money'. It is of relevance to note for present purposes that by virtue of Section 130(2) the definition extends to 'intangible information, IT data or video recording on a technical medium'.

Although the wording utilised in the CC differs from that in the FATF Glossary the evaluation team accepts the assurances of the Slovak authorities that, properly construed, the former now fully covers the latter.

Criterion 3.5 – The 2011 MER accepted, notwithstanding the then lack of information about autonomous ML convictions, that there was no legal requirement that a person be convicted of a predicate offence (para.51). Amendments to Section 233(1) of the CC, brought about by Act 397/2015 are consistent with and reinforce that conclusion.

Criterion 3.6 – The ML offence in Section 233 CC does not explicitly address the issue of extraterritorial predicate offences. Notwithstanding that, the authorities pointed to several sections of the CC of general applicability, together with the above-mentioned change in wording in Section 233(1) as well as case law on ML relating to foreign predicates. The AT accept this argument which was confirmed on-site.

Criterion 3.7 – The 2011 MER concluded that self-laundering was criminalised under Section 233 of the CC (para.54) and this conclusion has not been negated by subsequent legislative amendment in the SR. Furthermore, the Slovak authorities have provided examples of convictions obtained for self-laundering**.**

Notwithstanding this, as noted under Criterion 3.1 above, not ML acts committed by the perpetrator of the predicate crime without any demonstrable intent to conceal are not criminalised. This limits the scope of the self-laundering and does not fully meet the Conventions.

Criterion 3.8 – There is no specific legislative provision in the SR that the mental element of the offence may be inferred from objective factual circumstances, however this is implicitly recognised in the language of the Code of Criminal Procedure Code (CCP Section 2 para.12). Jurisprudence in this respect was already recognised by the previous evaluation report.

Criterion 3.9 – Under Section 233 of the CC, the money laundering provision, conviction carries a sentence of between two and five years of imprisonment. In determining the exact sentence to impose the courts will take cognisance of Division II of the CC entitled *'Fundamental Principles Applying to the Imposition of Sanctions'* being Sections 34 to 45 thereof.

Section 233 then provides for a series of more significant sanctions depending on the presence of what may be described as aggravating factors. The most exacting sentences, provided for in s.233(4), are imprisonment of twelve to twenty years. This tariff is triggered if the offender obtains 'a benefit of a large extent' for himself or another; if the offence is related to trafficking in drugs, nuclear or high-risk chemical substances, weapons or persons, or 'from another particularly serious crime'; or if the offender commits the offence as a member of a 'dangerous group'. Under the terms of Section 141 CC such a dangerous group includes both a criminal group and a terrorist group. The range of penalties are both proportionate and potentially dissuasive.

Criterion 3.10 – The SR first introduced a form of criminal liability for legal persons by Act 224/2010. Subsequently the Act on criminal liability of legal entities was passed and entered into force (Act 91/2016). This Act is a *lex specialis* in relation to the PC and the Code of Criminal Procedure.

Section 3 Act 91/2016 applies to a broad range of offences, including those relating to ML discussed above. It appears that the liability of legal persons under this enactment is without prejudice to the criminal liability of natural persons (see, eg, s.4(4)).

A broad range of sanctions – from the cancellation of a legal entity, forfeiture of a *"thing"*, pecuniary penalty, prohibition to undertake certain activities, prohibition to accept subsidies or subventions, to the publication of the conviction – is provided for (Section 10). These penalties may, with limited exceptions, be imposed separately or concurrently (Section 11(4)) and statutory guidelines are incorporated (see generally, s.11). Pecuniary penalties range from EUR 1,500 to EUR 1,600,000. In the abstract the regime of penalties appears to be proportionate and potentially dissuasive.

Criterion 3.11 – As already stated in the 2011 MER, the requirements of the EC are generally satisfied by Sections 13-14 and 19-21 of the CC (para.55). However, Section 13, which refers to conspiracy, relates only to conspiracy to commit a *"crime"*, which is defined in Section 11 as a criminal offence bearing a sentence of longer than five years. Under Section 233, the basic money laundering offence, in the absence of aggravating circumstances, bears of sentence of two to five years. It would therefore seem that conspiracy to commit a basic money laundering offence is not criminalised under Section 13. However, this largely offset by the approach to association in the CC including Art. 296.

Weighting and Conclusion

The SR has criminalized the fundamental aspects of ML. Minor shortcomings remain in relation to: the gap between the approach of the Conventions to the issue of the purposive element and coverage afforded by the interaction of Sections 231 and 233 of the CC with limitations to the criminalization of self-laundering; and conspiracy to commit a basic money laundering offence is not criminalised, although generally covered by the approach to association in the CC including Art. 296. **R.3 is rated Largely Compliant (LC).**

Recommendation 4 - Confiscation and provisional measures

Slovakia was rated Partially Compliant for the former Recommendation 3 in the 2011 MER. Technical deficiencies identified concerned the lack of sufficient provisions for protecting the rights of bona fide third parties and the lack of a clear authority to take steps to prevent or void actions in the sense of the then EC.3.6 (now C.4.2.c). The insufficient coverage of the confiscation of indirect proceeds for ML offences was mentioned as another shortcoming which, however, seems to have been properly and expressly covered already at the time of the previous evaluation by Art. 60(4) CC then in force (now Art. 130[1]e). Among the factors underlying the rating, it was only noted as an issue of effectiveness that the relevant provisions for confiscation from third parties were not used in a sufficient manner in practice – but as the body of the report made it clear that there were actually no clear and explicit legal provisions governing this area, this needs to be considered partly as a technical deficiency. The legal framework of the confiscation and provisional measures regime remained generally the same, apart from a few amendments, the most important of which was the extension and specification of the definition of *"thing"* in the CC.

Criterion 4.1 – The confiscation regime, as at the time of the 2011 MER, is based on three main legal instruments: the forfeiture of property (Art. 58 CC and for corporate entities, Art. 13 of the Law on Criminal Liability of Legal Entities) the forfeiture of a *"thing"* (Art. 60 CC being entirely applicable also to legal entities pursuant to Art. 14 of the aforementioned law) and the confiscation of a *"thing"* (Art. 83 CC).

Out of these, the forfeiture of property is a criminal sanction consisting of the confiscation of the entire property of the defendant, without any further specification, which is undoubtedly a robust measure targeting ill-gotten assets, but its generic and all-inclusive character makes it difficult to be tested against the more specific FATF standards in this field. In contrast, the forfeiture of a thing is a measure that corresponds to the FATF concept and definition of confiscation, extending to instrumentalities, intended instrumentalities and proceeds alike. The confiscation of a thing is an *in*

rem confiscation measure applicable to the exactly same scope of property items as above in cases the forfeiture of a thing could not be imposed.

While forfeiture of a *"thing"* can only be applied to items that belong to the perpetrator (see Art. 60(4) CC) the confiscation of an item, as a substitute measure to the former, can be applied to a third party provided that the item in question constitutes proceeds of crime or it was acquired in exchange for an item that constituted proceeds of crime. As a consequence, instrumentalities or intended instrumentalities of crime cannot be confiscated from third persons.

a) Although the 4th round MER concluded that the legal provisions being in force at that time (which are basically identical, at least in this sense, to the current legislation) provided for the confiscation of property that has been laundered, this conclusion needs to be reconsidered. The property that has been laundered (the body or *corpus delicti* of the ML offence) is not covered expressly by the confiscation and provisional measures regime, which may raise doubts whether it can adequately be targeted, particularly in classic 3rd-party ML schemes, by measures mentioned below under C.4.1(b). The case examples presented by the authorities, however, appear to demonstrate that such property can be subject to seizure and confiscation (as proceeds of crime) by broad interpretation of the existing legal framework.

b) Confiscation of proceeds of crime is clearly covered by the forfeiture of a *"thing"* (Art. 60(1)(c) CC) which refers, among others, to *"things"* the offender acquired through a criminal offence, and the definition of a *"thing"* expressly includes proceeds from any criminal activity as well as profit, interest and other benefits arisen from such proceeds (Art. 130(1)(e) CC). In addition, the forfeiture of property (Art. 58 CC) also extends to proceeds, but only indirectly, as the scope of this measure covers the entire property of the defendant, including illicit and legitimate assets alike (and in certain cases, it can be applied without proving the acquirement of any actual proceeds) so it is less compatible with the standards of R.4. Instrumentalities used or intended for use in any criminal offence are expressly covered by the forfeiture of a thing in Art. 60 paragraphs (1) a and (1) b CC. As noted above, the scope of the measures under Art. 60 CC is extended beyond property belonging to the perpetrator by means of the in rem confiscation provided under Art. 83 CC (except for instrumentalities).

c) As far as C.4.1(c) is covered, the Slovakian authorities opined that property used in, or intended or allocated for use in TF would be considered as instrumentalities and thus covered by Art. 60 paragraphs (1)a and (1)b CC. While this interpretation leave some room for doubt (such property can also be considered as the corpus delicti of the TF offence) the AT acknowledge that any FT-related property that cannot be forfeited, for any reason, pursuant to Art. 60 will necessarily be subject to confiscation under Art. 83(1)f CC which covers any property that "could be a source of financing terrorism".

d) Art. 60(2) CC allows for confiscating the equivalent value of the thing (proceeds, instrumentalities etc.) that is to be forfeited under Art. 60(1) if the original property item is inaccessible (i.e. hidden or transferred to someone else) unidentifiable or merged with the lawful property of the defendant or another bona fide person. A similar mechanism applies to things to be confiscated under Art. 83(1) CC as provided in Art. 83(4).

Criterion 4.2 – a) Law enforcement and prosecuting authorities have broad powers to identify property which is subject to confiscation. This includes general powers to obtain information from the available databases as well as from public authorities and other legal or natural persons pursuant to Art. 3 CCP. The latter extends to information subject to trade secrecy, banking secrecy or tax secrecy, or information from the records of registered securities if required by the court or by the public prosecutor in the preliminary stage of proceedings. There is however no centralised register of bank account holders, nor a clear and directly applicable provision to allow for the

monitoring of activity in bank accounts[58] . These measures are accompanied by coercive measures such as personal and house search and a variety of special investigative measures including controlled delivery and others. Any property/thing is valued on the basis of expert opinions or expert statements pursuant to the CCP.

b) The regime of the provisional measures has not significantly changed since the 4th round of MONEYVAL evaluation, when the then EC.3.2 and 3.3 were found to be in line with the FATF standards of that time. Seizure of things that are important for the criminal proceedings is provided by Art. 91 CCP. Pursuant to the Commentary to the CCP, the scope of this measure encompasses objects which may be considered as evidence as well as those that can be forfeited (Art. 60. CCP) or confiscated (Art. 83 CC) as proceeds of crime or instrumentalities. Seizure (freezing) of funds in a bank account as well as book-entry securities used to commit or intended for committing a criminal offence or constituting proceeds of crime is covered by Art. 95 and 96 CCP. Provisional measures applicable to the property of the defendant can be found in Art. 425 CCP (seizure for the enforcement of the forfeiture of property) and Art. 428 (seizure for the enforcement of forfeiture of a thing). All these measures can be ordered by the court or, in the preliminary stage of the proceedings, by the public prosecutor upon subsequent confirmation by the court. While the measures in Art. 95 and 96 CCP are to be applied *ex parte* and without prior notice (see e.g. Art. 95[6]) the same does not seem to apply to objects to be seized under Art. 91 CCP as this measure must be preceded by an action where the possessor of the respective item is formally prompted to hand it over to the authorities. Seizure of funds and bonded securities under Art. 95 and 96 CCP are applicable also to third parties (even if the former refers to third-party owners while the latter to third-party holders) which does not seem to be the case for seizure of things under Art. 91. The provisional measures in Art. 425 to 428 CCP can only be applied to the defendant and only in cases there is a concern that the enforcement of the respective forfeiture measure will be impeded or obstructed (otherwise the general rules for seizure apply). Seizure for the purposes of confiscation of a thing is provided under Art. 461 CCP which, by nature of the said confiscation measure, applies to third persons too.

c) Art. 426(2) CCP provides as a general rule that all legal actions of the defendant are invalid (and hence voided by law) that relate to the property seized with a view to its forfeiture pursuant to Art. 58 CC. A similar provision can be found in Art. 95 (7) CCP regarding funds that have been seized. There is however no general provision available in this field and therefore property items seized pursuant to Art. 428 and 461 CCP with a view to their forfeiture under Art. 60 or Art. 83 CCP respectively, appear to remain uncovered. The Slovakian authorities claim that Art. 95 (7) would necessarily apply to both Art. 428 and 461 CCP as these make reference to a number of other CCP articles, including Art. 95 CCP, as providing for general procedural rules. Considering however that Art. 95 CCP is restricted to funds in the form of bank account money, Art. 95 (7) does not seem to be interpretable in a general manner, extending to all forms of property or property items.

d) Appropriate investigative measures are provided for by the CCP (see more in details under Recommendation 31).

Criterion 4.3 – Protection of the right of bona fide third parties is determined by the relatively narrow scope in which third party confiscation can take place in Slovakia. Namely, forfeiture of property and forfeiture of a thing can only be applied to the property or items of the defendant (in case the defendant's property is merged with that of a bona fide third person, the value equivalent of the respective property will be confiscated). Third parties' rights can however be affected by the *in rem* confiscation measures in Art. 83 paragraph (1)c and (1)d CC.

---

58 In lack of the latter, the Slovakian authorities rely on the combination of the AML/CFT Act (which empowers the FIU to perform monitoring of suspicious financial transactions) and the rules of mandatory cooperation in criminal proceedings pursuant to Art. 3 CCP although this has never been tested in practice.

As far as provisional measures are concerned, legitimate interests of third parties are protected by procedural rights to participate in the proceedings (Art. 45 CCP see analysed in the 4th round MER[59]) to request the revocation or restriction of the seizure of funds or booked securities (Art. 95 [8] and 96 [3] CCP) to lodge a complaint against prosecutorial decisions on seizure of assets (Art. 191 CCP) and to appeal against a decision to secure the execution of a sentence of the forfeiture of property or that of a thing (Art. 425 and 428 CCP respectively).

Despite the breadth of procedural rights provided for bona fide third parties, there is no positive protection in substantive law for parties with legitimate rights to property items subject to seizure or forfeiture (such as a general provision that these measures shall be applied without prejudice to the legitimate interests of third parties having acquired the respective property item in good faith) in lack of which the *bona fide* purchaser could only seek compensation from the perpetrator. This legislative gap was, to a certain extent, filled by the Constitutional Court which ruled in 2016 that the property rights of the *bona fide* acquirer are to be granted constitutional protection, which must be considered and carefully assessed by the general courts[60].

Criterion 4.4 – There is are various mechanisms for managing and/or disposing of property that is seized or confiscated without a centralized body in charge of management of such property. Seized property is held in safekeeping by the respective authority (police body, prosecutor's office or court) that carried out the seizure. If these are not able to do so, the safekeeping may be provided through another public body or legal person or natural person doing business in that sector. In case of real estate, the said authorities may authorize a person to administer the property (Art. 94 CCP) but there are no rules to provide for the management of seized property beyond safekeeping measures. As far as confiscated/forfeited property is concerned, there are various regimes available, depending on whether the entire property of a defendant was forfeited under Art. 58 CC or specific items pursuant to Art. 60 or Art 83 CC. In the first case, the competent bankruptcy court sends the judgment, immediately after it has become enforceable, to the bankruptcy trustee who shall sell the relevant property by public auction pursuant to the Bankruptcy Act. In case of forfeiture of a thing, the judgment is sent to the District Office that is, the government authority administering the State's property which will take over the property and disposes of it according to the Law 278/1993 on the management of the assets of the State so that the items be either used by the State, sold by tender or liquidated (destroyed). Neither of these pieces of legislation appear to provide for active management of property or property items beyond safekeeping measures until they are disposed.

Weighting and Conclusion

Apart from slight changes in the legislation, the provisional measures and confiscation regime remained largely the same as it was at the time of the 4th round MONEYVAL evaluation. As a consequence, deficiencies noted at that time such as the lack of clear provisions in substantive law for protecting the rights of bona fide third persons and the lack of a clear authority to take steps to prevent or void actions in the sense of C.4.2.c remained largely valid. Confiscation of laundered property does not seem to be expressly covered by law and the coverage of third-party confiscation is still incomplete. Management of seized and confiscated assets until their disposal is provided for but does not seem to extend beyond safekeeping measures. **R.4 is rated LC.**

[59] See para 131 on page 46.

[60] See decision I. US 549/2015-33. The Constitutional Court ruled in relation to a bankruptcy case but the constitutional principles invoked in the decision are of an overarching nature and thus are also relevant in the context of FATF Recommendation 4.

Recommendation 5 - Terrorist financing offence

Special Recommendation II was rated PC in the 2011 MER of the Slovak Republic. In addition to effectiveness concerns, which are addressed elsewhere in this evaluation, there were two factors underlying this rating. First, the absence of full criminalisation of the financing of the individual terrorist's day to day activities. Second, the non-criminalisation of the financing of the acts defined in the treaties annexed to the TF Convention.

While Recommendation 5 of the current FATF standards both amends and restructures former SR II it continues to adopt the same major thrust. The SR has sought to address the identified deficiencies and new FATF requirements primarily through amendments to its Criminal Code (CC).

Criterion 5.1 – The TF Convention entered into force, without reservations, for the SR on 13 October 2002. In an innovation introduced since the 2011 MER the CC of the SR now contains a free-standing provision in this area. Section 419c, entitled 'Terrorist Financing', has clearly been influenced by Article 2 of the TF Convention and related international standards. The criminal offence of terrorism is defined in Section 140b of the CC. In addition to terrorist financing, this includes establishment, plotting and supporting a terrorist group (s.297), terror (ss 313-314), terrorist attack (s. 419), certain forms of participation in terrorism (s.419b), and, travelling for the purpose of terrorism (s.419d). Section 140(d) is also of relevance in this context.

In the view of the AT the interaction of the above provisions satisfy the requirements of Article 2(1)(b) of the TF Convention. While the SR is a party to all of the Conventions in question and the CC criminalises the offences contained therein, this is not, in and of itself, sufficient to satisfy the requirements of Article 2(1)(a). It is acknowledged that the wording of Section 419 ('Terrorist Attack') has drawn inspiration from these international instruments, particularly, in paragraph 1. However, there remains a requirement to prove an intention 'to damage the constitutional establishment or defensibility of a country…' etc. This is not in conformity with the FATF standard.

Criterion 5.2 – As discussed in relation to c.5.1 above, the CC of the SR now establishes the financing of terrorism (Section 419c) as a separate criminal offence. The offence can be committed directly or 'through another person' (para.1). It applies to a person who 'collects or provides, directly or indirectly, items, funds or other means for a terrorist offender, for a terrorist group or a member thereof or for committing any of the criminal offences of terrorism…'. The provision also applies to such 'collection' with the intention that they may be used for such a purpose or with the knowledge that they may be used for such a purpose…' (para.1).

This key provision must, in turn, be read in the light of other relevant sections of the CC. In particular, and as discussed under c.5.1, Section 140b defines 'criminal offences of terrorism' in a broad fashion. Furthermore, Section 129 addresses, *inter alia*, terrorist groups (para5) and the provision of support (including financial support) thereto. Membership of a terrorist group and the provision of support to such a group are criminalised by Section 297 of the CC.

Criterion 5.2bis – By virtue of Section 419d of the CC travel for the purpose of terrorism is criminalised in the SR and the Terrorism Financing offence (s.419c) applies thereto. The same holds in respect of the provision and receipt of terrorist training criminalised under Section 419b(2) of the CC. It is of relevance to note for present purposes that preparation and planning are also criminalised in the SR (see, eg, PC, ss 13-14).

Criterion 5.3 – This criterion requires the TF offence to extend to 'any funds or other assets'; terminology very broadly defined in the Glossary to the FATF Recommendations. Section 419c of the CC, utilises the term 'items, funds or other means'. Section 419c of the CC does not, in terms,

distinguish between funds or other assets from legitimate or illegitimate sources and the SR holds to the view that both are consequently covered by the wording. I support of that view, Art. 130 of the CC defines the "item" as: "*a) a movable item or immovable item, residential or non-residential premises, … b… c)… d…. e) proceeds from a criminal activity as well as the profit, interest and other benefits arisen from such proceeds*,". Since letter e) specifically identifies *"proceeds"* as part of the definition of *"item",* the AT is satisfied that both *"legitimate"* and *"illegitimate"* sources are covered.

Criterion 5.4 – Section 419c does not explicitly require that funds or other assets are actually used to carry out or attempt a terrorist act or be linked to a specific terrorist act.

Criterion 5.5 – Under the applicable international standard it should be possible for the intent and knowledge required to prove the TF offence to be inferred from objective factual circumstances. This issue is not directly addressed in Section 419c. However, for the reasons set out in the discussion of c.3.8 above, this criterion can be regarded as being satisfied in the legal system of the SR.

Criterion 5.6 – The basic tariff for the commission of a TF offence in the SR is 'a prison sentence of five to fifteen years' (Section 419c(1) and (2)). However, if committed 'to a large extent' – at least EUR113,000 – or 'as a member of a dangerous group' –which under CC s.141 includes a terrorist group- the severity of the sanctions is increased to a prison sentence of 10 to 20 years. Viewed in the abstract these penalties appear to be both proportionate and potentially dissuasive.

Criterion 5.7 – The Act on criminal liability of legal entities was passed and entered into force in 2016 (Act 91/2016). This Act is a *lex specialis* in relation to the CC and the Code of Criminal Procedure.

Under Section 3 Act 91/2016 applies to a broad range of offences, including, inter alia, terrorist financing. The liability of legal persons under this enactment is without prejudice to the criminal liability of natural persons (see, eg, s.4(4)).

A broad range of sanctions – from the cancellation of a legal entity to the publication of the decision of conviction – is provided for (Section 10). These penalties may, with limited exceptions, be imposed separately or concurrently (Section 11(4)) and statutory guidelines are incorporated (see generally s.11). In the abstract the regime of penalties appears to be both proportionate and potentially dissuasive.

Criterion 5.8 – As noted in the context of the earlier discussion of money laundering, the legal system of the SR makes appropriate provision for ancillary offences (see c.3.11; see also, s.419c(2) of the CC).

Criterion 5.9 – As the SR adopts, as noted in the discussion of Recommendation 3 above, an 'all crimes' approach the Financing of Terrorism, as defined in Section 419c, constitutes a predicate offence for money laundering.

Criterion 5.10 – In the absence of any relevant limitation in Section 419c of the CC, or more generally, the evaluators share the view of the Slovak authorities that this offence applies regardless of whether or not the alleged perpetrator is in the same country or a different country from the one in which the terrorist or terrorist organisation is located or the terrorist act occurred or will occur.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, minor deficiency remains in relation to the requirement to prove an intention *'to damage the constitutional establishment or defensibility of a country…'*. **R.5 is rated Largely C**.

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

Special Recommendation III was rated PC in the 2011 MER of the Slovak Republic. Certain of the factors underlying this rating related to perceived deficiencies in the EU instruments transposing UNSCR's into European Law and the timelines of designations under EU processes. In addition, the 2011 MER noted several further factors as contributors to the overall rating: the lack of any national mechanism to consider requests for freezing from other countries; insufficient guidance and communication mechanisms with financial institutions (except banks) and DNFBPs regarding designations and instructions including asset freezing; lack of clear and publicly known procedures for de-listing and unfreezing in appropriate cases in a timely manner; and, insufficient monitoring for compliance of financial institutions and DNFBPs.

Criterion 6.1 – The SR implements targeted financial sanctions pursuant to UNSCR 1267 and 1988 (on Afghanistan) – through Regulation (EU) 753/2011 and Council Decision 2011/486/CFSP and UNSCR 1267/1989 (on Al Qaeda) – through Regulation (EU) 881/2002 (and successors) and Council Decision 2016/1693/CFSP (replacing the Common Position 2002/402/CFSP), which have direct effect in all EU member states. These EU measures interact with and are supplemented by national legislation, namely the International Sanctions Act 289/2016 (ISA) on the implementation of International Sanctions as amended.

a) According to Art. 16 (8) of the ISA, the proposal for inclusion of an individual in the list of sanctioned persons shall be sent by the MFA to the competent institution or the UN department. The proposal is filed in the form and manner stipulated by the relevant resolutions of the UNSC, or binding acts of the EU.

b) The mechanism for identifying targets for designation is described under Art 16 (2) of the ISA. The proceeding shall be initiated by the competent state administration authority, SIS, Military Intelligence, law enforcement authorities, or other individual, or without the need of such proposal, if the competent state administration authority gained knowledge based on its own activity justifying the initiation of the proceeding. The designation criteria as set out in the relevant UNSCR are absent.

(c) – Article 16(3) of the International Sanctions Act sets out the relevant criteria to be satisfied in the context of designations. This is framed in terms of *'a description of the facts justifying the suspicion…'*. This amounts to a *"reasonable basis"* required by the standard. Proposals for designation are not conditional upon the existence of criminal proceedings.

(d) - The proposal is filed in the form and manner stipulated by the relevant resolutions of the United Nations Security Council, or binding acts of the European Union.

(e) - The decision concerning the proposal for inclusion of an individual in the list of sanctions shall contain all the information required by 6.1(e).

Criterion 6.2 – The SR implements UNSCR 1373 principally through EU Council Regulation 2580/2001 and EU Council Common Positions 2001/931/CFSP and the International Sanctions Act.

(a) – At the EU level the Working Party on restrictive measures to combat terrorism (COMET WP) uses a *'reasonable basis'* evidentiary standard, and designation is not conditional on the existence

of criminal proceedings. At the national level, there is no one single designated authority, but all state administration authorities/ministries according to the Competence Act No. 575/2001 are responsible to designate in the area of international sanctions. There is a group of ministries and state authorities[61] that review and assess any proposal for listing/delisting in the process of preparation of a proposal for designation. The ISA also establishes arrangements and procedures for the receipt and verification of designation requests received from third countries (See, eg, Article 16a)

(b) – At EU level, identification of designation targets is covered by CP 2001/931/CFSP. At domestic level the ISA creates a system for the "Autonomous Declaration of International Sanctions" (Art.3) which is relevance for designations under UNSCR1373. The legislation of the SR articulates a procedure for proposing to the EU an individual for inclusion on its relevant list of sanctioned persons. Such proposals are to be transmitted by the MFA to the relevant working group (Art.16 of the ISA).

(c, d) – The COMET WP assesses, at the EU level, whether any listing request meets the designation criteria and other requirements under Common Position 2001/931/CFSP. It also makes decisions as to recommendations to be made to the European Council based on reliable and credible evidence without it being conditional on the existence of an investigation, prosecution or conviction. In the ISA, the requirements are the identification of the person and the satisfaction of a *'suspicion'* based test (Art.16a(3)(b)) which is in line with the requirements under C.6.2(c,d).

(e) At the European level there is no specific mechanism that would allow for requests to non-EU member countries to give effect to the EU list. At the national level there is no formalised procedure under which Slovakia could ask another country to give effect to freezing measures but in the same time, there is nothing in the International Sanctions Act which would preclude the making of requests to third countries, if need be.

Criterion 6.3 – (a) – At European level, all EU member states are required to provide each other with the widest possible range of police and judicial assistance on TFS matters, inform each other of any actions taken, cooperate and supply information to the relevant UNSC bodies (Art.8 Reg.881/2002; Art.8 Reg.2580/2001; Art.4 CP 2001/931/CFSP). At national level Art. 19 of the International Sanctions Act makes detailed provision for the gathering of information and data for purposes connected with the implementation of, *inter alia*, targeted international sanctions.

(b) – Designations at the European level take place without prior notice to the person/entity identified (EC Regulation 1286/2009 preamble para.5). The EU Court of Justice makes an exception to the general rule that notice must be given before the decision is taken in order not to compromise the effectiveness of the first freezing order. At the level of the domestic law of the SR Article 24(4) of the International Sanctions Act provides as follows: *'The person who is proposed to be included in the list of sanctioned persons shall not be a party to the proceedings concerning the filing of a proposal for inclusion of an individual in the list of sanctioned persons in accordance with Article 16 and 16a'*. (See also, Art.4(5)).

Criterion 6.4 – The EU procedure in respect of designations made by the relevant Committees of the UNSC implies a delay between the date of a designation by the UN and the date of its transposition into European law under Regulations 881/2002 and 753/2011 respectively, because of the time taken to consult between European Commission departments and translate the designation into all official EU languages. Thus, implementation of targeted financial sanctions

[61] MoI, MoF, Ministry of Defence, MoFA, SIS, Militari Intelligence.

pursuant to UNSCRs 1267/1989 and 1998, does not occur *'without delay' i.e.*, ideally within hours as required by the FATF standards. This deficiency is diminished as a result of the application of the ISA.

More precisely, Art. 15 of the ISA includes a new provision which obliges the MFA to publish on its website references to the relevant UNSCRs (para. 5) and successive designations made pursuant thereto *'without any undue delay after they are adopted'* (para.6). Furthermore, obligated entities are required to carry out effective measures to monitor lists of sanctioned persons and prevent disposal of the property of the sanctioned person' (Art.4(3, 5)). This legislation appears to carry, as a matter of international law, the authority of Article 41 of the UN Charter. Nevertheless, this interpretation is contradicted by the guidance issued in 2019 to obligated entities by the MoF of the SR entitled "*Procedures for Effective Implementation of Rules and Procedures for Freezing Funds and Assets of Terrorist and Other Persons in the Conditions of the Slovak Republic",* which provides that if the UNSC adopts a resolution in the area of restrictive measures against natural persons or legal entities,such Resolution is transposed to the EU Regulations of the EP and of the Council EU. . The Slovak authorities recognised that this was a not-intended discrepancy and invoked the higher legal hierarchy borne by the ISA[62]. The AT agrees with this argument and concludes that the requirement is met.

Targeted financial sanctions related to UNSCR 1373 are implemented by Council regulations (Regulation 2580/2001) that are implemented directly in the Slovak legal framework. These sanctions are thus implemented *'without delay'*.

Criterion 6.5 – (a) – Natural and legal persons in the SR are required to freeze funds and other assets under UNSCRs 1267/1989 and 1988 only when such obligations have been transposed into the EU legal framework. As noted in c.6.4 above such designations are not so transposed without delay. While under the International Sanctions Act freezing action formally takes place without prior notice, the time lag between designation by the UN and required action by the EU affords, in practice, listed persons an opportunity to take action to move or otherwise protect funds or assets at risk.

Under UNSCR 1373, the obligation to freeze funds and other assets applies immediately in all EU member states because of the direct legal effect of the relevant EU instruments. However, under Council CP 2001/931/CFSP listed EU *'internals'* are not subject to freezing measures but only to increased police and judicial cooperation among members. Accordingly, the freezing without delay and without prior notice of the funds and other asserts of EU *'internals'* is a matter for national law and policy. The process of listing through the "Ordinance of the Government of the SR declaring the international sanction against EU internals" is included in the Art. 16a of the International Sanctions Act.

(b) – Pursuant to UNSCRs 1267/1989 and 1988, the freezing obligation extends to all funds and other assets that belong to, are owned, held or controlled by a designated person or entity. The obligation to freeze the funds or assets of persons and entities acting on behalf of, or at the direction of designated persons or entities is covered by the notion of *'control'* in Regulations 881/2002, and 753/2011. Further amendments were introduced into the EU legal framework in 2016 which ensure conformity with FATF requirements in this context (See, Council Decision (CFSP) 2016/1693 and Council Regulation (EU) 2016/1686).

[62] Shortly after the on-site the wording of the "Procedures" was changed to provide direct legal effect of UNSC resolutions/decisions in the Slovak Republic.

By virtue of Article 2(i) of the ISA *'sanctioned property means property possessed, held or otherwise controlled by a sanctioned person or controlled, directly or indirectly, by a sanctioned person or a person acting in favour of a sanctioned person, or any other property to which an international sanction applies'*. This provision, when considered along with the broad definition of *'property'* in Article 2(h) would appear to provide an appropriate basis to satisfy the relevant FATF requirements in this context.

(c) – At the EU level, and in a manner consistent with the UNSCRs, relevant Regulations prohibit EU nationals and persons within the EU making funds and other assets available to designated persons and entities. The provisions of the International Sanctions Act (Art. 4 (5)) set out national framework for prohibitions, which are sufficiently broad to cover the requirements as provided under the FATF Recommendations.

(d) – Designations decided at the European level are published in the Official Journal of the EU and website and included in a consolidated financial sanctions database maintained by the European Commission, with an RSS feed. The EU Council provides guidance by means of the EU Best Practices for the effective implementation of restrictive measures.

At national level, Article 4(3) of the International Sanctions Act places the onus upon obligated authorities and entities *'to carry out effective measures which would allow them to monitor lists of sanctioned persons'*. In Art. 2(u) a definition of *'list of sanctioned persons'* is provided along with the statement that such lists *'are published in the Official Journal of the European Union or in the collection of Laws of the Slovak Republic'*. As noted earlier in the discussion of c.6.4, Article 15(5) and (6) of the same enactment requires the MFA to publish on its website relevant UNSCRs and designations; the latter 'without any undue delay after they are adopted'.

In addition to the above, the Ministry of Finance issued in 2019 a guidance paper ("Procedures for the effective implementation of rules and procedures for freezing funds and assets of terrorists and other persons in the practice of the SR") the purpose of which *'is to instruct the entities in the financial market in what to do when they identify during their day to day work individuals, payment transactions or assets which are subject to international sanctions'.* This includes details of the websites which obligated entities are expected to monitor in the discharge of their legal obligations. No information on additional initiatives or those that might be tailored to DNFBPs have been provided to the AT.

(e) – Natural and legal persons (including FIs/DNFBPs) are required to provide immediately to the designated national authority (Ministry of Finance) any information about accounts and amounts frozen under EU legislation per articles 5.1 of EU Regulation 881/2002, 4 of EU Regulation 2580/2001, and 8 of EU Regulation 753/2011.

At the national level, under Article 4(5) of the ISA, if an obligated entity *'finds out, or has a suspicion, that property of sanctioned persons is registered or kept by it, it shall be obliged to immediately prevent disposal of the property of the sanctioned person' and to notify the relevant state authority of the action taken 'without undue delay'*. (See also, Art 91(8) of the Act on Banks: Act No. 483/2001). Since there is no reference to "transactions" but to property the "attempted transactions" are covered.

(f) – The relevant EU legal framework makes some provision for the protection of bona fide third parties (see, eg, Reg. 881/2002, Art.6; Reg. 753/2001, Art.7; Reg.2580/2001, Art.4). Such provision is not explicitly included in the International Sanctions Act or in the Act on Administrative Proceedings (No. 71/1967 Coll.). However, Code of Judicial Administrative Procedures No. 162/2015 in Art.2 par. 2 states that anyone who claims that his rights or legally

protected interests have been violated or directly affected by a decision of a public authority, action by a public authority, inaction of a public authority or other intervention by a public authority may, under the conditions laid down by this Act, seek protection before the administrative court.

Criterion 6.6 – (a-e) – The ISA contains detailed provisions relating to the delisting and unfreezing of funds or other assets of persons and entities which do not, or no longer, meet the criteria for designation. These are in turn summarised in the 2019 guidance issued by the Ministry of Finance *("Procedures for the effective implementation of rules and procedures for freezing funds and assets of terrorists and other persons in the practice of the SR"*).

In so far as designations arise from actions taken at either the UN or EU level, the International Sanctions Act entertains two possibilities. First, Article 17 establishes a mechanism through which the SR itself may make a proposal for delisting and any resulting proposal to this effect shall be sent by the MFA to the relevant UN or EU authorities in such manner and form as is required by them. The sanctioned person may lodge an application to initiate such proceedings, (Art. 8(2)). The same person is afforded a right of appeal against a decision not to submit a proposal for delisting under this process (Art.17(5)). Second, Article 18(3) makes it clear that a sanctioned person may apply direct to the appropriate UN and EU mechanisms to seek delisting.

Designated persons and entities may also challenge the EU act imposing relevant sanctions by instituting proceedings (according to Art.263, para.4 and Art.275, para.2 TFEU) before the EU Court of Justice, regardless of whether the designation was initiated by the EU on its own motion, or pursuant to UN sanctions.

(f-g) – EU Best Practices for the effective implementation of restrictive measures provide publicly known procedures for obtaining assistance for verifying whether persons or entities having the same or similar name as designated persons or entities (i.e. a false positive) are inadvertently affected by a freezing measure. Article 18(4), to be read in conjunction with Article 14, of the International Sanctions Act addresses the same issue. The legislation of the SR also treats the issue of the revocation of the seizure of property when the reasons giving rise to the same expire (Art.14(6)). De-listing and unfreezing decisions taken in accordance with European regulations are communicated to the REs by publication in the Official Journals of the EU and on a dedicated website.

Criterion 6.7 – Access to frozen funds and other assets is provided under Article 2a of EU Regulation 881/2002 and Articles 5-6 of EU Regulation 753/2011, which are directly applicable in the Slovak Republic. At national level such provisions are stipulated under Article 13 of Act 289/2016 entitled 'Exemptions from the Sanctions Regime'. This differs in its wording, and seemingly in its scope, from the relevant international instruments. More precisely, Art. 13 (1) provides a series of cases for which the provisions of the ISA do not apply such as: i) humanitarian aid, unless it is restricted by a special regulation, ii) financial contribution to compensate for the social consequences of a severe disability, replacement maintenance, social insurance benefit, social security benefit, iii) wage, wage compensation, redundancy payment or any other payment following from labour relations; iv) social insurance premium and contribution for old-age pension saving; v) alimony. However, EU restrictive measures, whether implementing UN TFS or setting up autonomous sanctions, are directly applicable to all EU operators. Thus, by virtue of Article 3(1) of Council Regulation (EU) No 753/2011 ('Afghanistan Regulation') and Article 2(1) of Council Regulation (EC) No 881/2002 ('Al-Qaida Regulation'), "all funds and economic resources belonging to, owned, held or controlled by a natural or legal person that are listed shall be frozen" which means that funds made available to a listed person can be transferred to their account but are

immediately frozen. Therefore, even if the ISA provisions are not strictly in line with UN TFS, any inconsistency would be corrected by the principle of conform interpretation of the national legislation, consecrated in EU law, as in accordance with this principle, the EU law takes precedence over national incompatible provisions, which need to be interpreted and applied in a way which respects EU legislation.

Weighting and Conclusion

There are some minor shortcomings related to the application of the requirements under Recommendation 6, in particular absence of designation criteria as set out in the relevant UNSCR, absence of formalised procedure at the national level under which Slovakia could ask another country to give effect to freezing measures, provision for the protection of bona fide third parties is not explicitly included in some Acts, insufficient level of communicating with the DNFBPs. Criteria 6.3, 6.4, 6.6 and 6.7 are Met. **R.6 is rated LC**.

Recommendation 7 – Targeted financial sanctions related to proliferation

These requirements were added to the FATF Recommendations in 2012 and were therefore not previously assessed. The sanctions regime in the Slovak Republic is regulated by relevant EU legislation and, at the national level, by the International Sanctions Act.

Criterion 7.1 – At the EU level, UNSCR 1718 and successor Resolutions on the Democratic People's Republic of Korea (DPRK) is transposed into the EU legal framework (the current legislative framework is based on Council Decision (CFSP) 2016/849 and Regulation (EU) 2017/1509)). UNSCR 2231 on Iran is transposed into the EU Legal framework through EC Regulation 267/2012 as amended by EC Regulations 2015/1861 and 1862. EU regulations and the UNCSRs are directly applicable in Slovakia, as explained under c.6.4.

Criterion 7.2 – a) Following the direct application of the relevant EU legislation, all natural and legal persons in the SR are required to freeze funds or other assets of designated persons and entities and must refrain from giving prior notice to designated persons/entities. Additionally, the ISA (Art. 4(2)(b)) establishes that individuals (which may be any natural person) which keep financial means, other property, goods or means of transport shall immediately prevent the disposal of the property of the sanctioned person.

b) The relevant EU legislation covers the requirement to freeze all types of funds or other assets as targeted by the FATF Methodology. As described in C.6.5, the definitions of 'sanctioned property' together with the definition of 'property' as set forward in the International Sanctions Act create a sufficiently wide scope of funds to be frozen.

c) The EU Regulations prohibit that any funds or other assets are being made available to designated persons, or for their benefit. On the national level the provisions of the ISA (Art. 4 (5)) set out national framework for prohibitions, which are sufficiently broad to cover the requirements as provided under the FATF Recommendations.

d) As described in C.6.5(d), implementing entities (i.e., those authorities and persons responsible for the implementation of international sanctions) are obliged to carry out measures to monitor the sanctions lists. The Ministry of Foreign and European Affairs publishes on its website, without undue delay after their adoption, references to relevant UNSCRs (currently these are 1718/2006 and 1737/2006, 1835/2008 and 2231/2015), although the website does not include all relevant successor resolutions or updates to the lists but refers to the main page of the UNSC. Moreover, the web page of the MFA redirects to the consolidated version of the sanctions lists so allows for comprehensive information on the sanctions in force and on the persons under sanctions regime.

Designations and updates of sanctions lists shall also be published in the Official Journal of the EU or in the collection of Laws of the Slovak Republic. The guidance paper which was published in 2019 by the Ministry of Finance for financial institutions on Procedures for the effective implementation of international sanctions also covered proliferation financing TFS. No guidance was published for the implementing entities which are not financial entities (such as public administration authorities, non-banking financial institutions, DNFBPs and natural persons).

e) Following the European legal framework, all persons are required to immediately provide the designated competent authority with information on any measures taken under the international sanctions regime (see C.6.5(e)). Besides, pursuant to the national legal framework, an implementing entity is obliged to inform the relevant competent authority on the measures adopted in case the entity has a suspicion or finds out that property of sanctioned persons is registered or kept by it (International Sanctions Act, Art 4(5)). Banks and branches of foreign banks are also required to regularly provide the relevant competent ministry with a list of clients subject to international sanctions (Act 483/2001 on banks, Art. 91(8)).

f) The rights of bona fide third parties are protected through the existing European Regulations (in particular, 2017/1509 (Art. 54) and 267/2012 (Art. 42)). Such provision is not explicitly included in the ISA or in the Act on Administrative Proceedings (No. 71/1967 Coll.). However, Code of Judicial Administrative Procedures No. 162/2015 in Art.2 par. 2 states that anyone who claims that his rights or legally protected interests have been violated or directly affected by a decision of a public authority, action by a public authority, inaction of a public authority or other intervention by a public authority may, under the conditions laid down by this Act, seek protection before the administrative court.

Criterion 7.3 **–** Under the EU Regulations 267/2012 (Art. 47) and 2017/1509 (Art. 55), EU Member States must take all necessary measures to implement EU regulations, which would include adopting measures to monitor compliance of the sanctions regime by FIs and DNFBPs. Failure to comply with the obligations flowing from the ISA may result in sanctions applicable to natural and legal persons (Arts. 21-23). The sanctions are of an administrative nature and range from EUR 109 up to EUR 66,400 for a 'person', depending on the type of offence, and EUR 50,000 up to EUR 132,800 for a legal entity or an individual-entrepreneur. The sanctions shall be determined by the competent state administration authority and the implementing authority or by the Ministry of Finance. There is no direct reference in the legislation to the obligation to *"monitor"* the compliance of FIs and DNFBPs with Recommendation 7.

Criterion 7.4 **–** As described in C.6.6, the International Sanctions Act contains detailed provisions on the procedures for de-listing and un-freezing of funds or other assets of persons and entities which do not, or no longer, meet the criteria for designation. These procedures are publicly known and in line with the de-listing procedure set forward in UNSCR 1730 (2006). Where the authorities make a proposal for de-listing to the UNSC, Art. 17 of the International Sanctions Act sets out that the Ministry of Foreign Affairs takes such steps based on the decision of the competent state administration authority, upon initiative of the procedure for exclusion by the competent authority, SIS, Military Intelligence, LEAs or other individual. Art. 18(4) of the International Sanctions Act further establishes that the mechanism described in Art. 17 shall be applied in case of a false-positive or whenever the reasons for an individual's inclusion in the list of sanctions persons have expired.

a) The EU Best Practices for the effective implementation of restrictive measures (4 May 2018) lay out the procedure for de-listing requests regarding UN sanctions. Petitioners of PF-related TFS can submit de-listing requests either through the Focal Point established pursuant to UNSCR 1730, or

through their government. If a person is de-listed from the UN sanctions list, relevant amendments are also made to the corresponding legal acts of the EU. Pursuant to the International Sanctions Act, an individual who is included in the list of sanctioned persons may directly apply with the UNSC for exclusion from this list (Art. 18(3)).

b) Besides the publicly known procedures to unfreeze the funds of persons and entities with the same or similar name as designated persons and entities at the EU level, the International Sanctions Act also foresees measures to be adopted by the competent authority in case of a false-positive (Art. 17). This article should be read in conjunction with Article 14 of the same Act, which prescribes the mechanism for (revocation of the decision of) seizure of property subject to international sanctions.

c) EU Regulations 2017/1509 (Arts. 36 and 37) and 267/2012 (Arts. 24, 26 and 27) authorise access to funds or other assets provided the conditions stated in UNSCR 1718 and 1737 are met. The ISA in Art. 13 further regulates exemptions from the sanctions regime, by way of access to the sanctioned financial means, upon request of the sanctioned person.

d) At European level, updates to the lists, including on de-listing and unfreezing actions, are published in the EU Official Journal, as soon as such actions are taken. At national level, decisions on unfreezing shall be communicated to persons who are affected by the decision (Art. 14(8), International Sanctions Act), however, there is no mentioning in the legislation that such publication shall take place within a certain timeframe. Updates to the list shall also be published on the website of the Ministry of Foreign Affairs (Art. 15(5)) and unfreezing decisions are communicated in written to financial institutions. According to the *"Procedures for the effective implementation of rules and procedures for freezing funds and assets of terrorists and other persons in the practice of the SR"* the implementing entities must be informed, but not obliged, of the sanctioned persons and sanctions lists and are expected to monitor the sanctioned persons lists. However, a clear mechanism to communicate decisions on de-listings to DNFBPs or to provide guidance to DNFBPs on their obligations to respect a de-listing or unfreezing action is not established. No proactive communication mechanisms appear to be in place in the SR.

Criterion 7.5 – The requirements are met through the European and national legal framework.

a) Regulated in the EU Legal framework (Regulations 2017/1509: Art. 36 and 267/201: Art. 29), it is permitted to add interests or other earnings to frozen accounts. This is also included in Art. 13(1) of the International Sanctions Act, which authorises additions to the accounts for humanitarian aid, social benefit, wage, social insurance premium and alimony under certain conditions.

b) Under EU Regulation 2015/1861 (amending Regulation 267/2012), Art. 25, it is permitted to make payments of the frozen account under a contract entered into prior to designation under certain conditions. The same is included in the ISA, Article 13(2), which states that a payment of a sanctioned person owed under a contract, agreement or obligation which was concluded or arose before the international sanction may be permitted. Nevertheless, Art. 13 of the International Sanctions Act does not clearly include a reference to the list of guarantees as set out in the FATF Methodology (C.7.5(b)(i-iii)). The protection against such cases may be inferred from the fact that a decision from the competent state authority is still needed for the operation to be executed.

Weighting and Conclusion

The SR meets most of the requirements of Recommendation 7. Minor shortcomings remain such as a certain lack of clarity in the establishment of the functions of the various state bodies in the PF

TFS field, no guidance for the implementing entities which are not financial entities, no direct reference in the legislation to the obligation to "monitor" the compliance of FIs and DNFBPs with Recommendation 7, as well as absence of a clear reference to the list of guarantees as set out in the FATF Methodology (C.7.5(b)(i-iii)). **R.7 is rated LC.**

Recommendation 8 – Non-profit organisations

In the 4th round of evaluations Slovakia was rated Non-Compliant with former Special Recommendation VIII. No risk assessment of NPOs has been undertaken, no review of the adequacy of legislation to prevent the abuse of NPOs for TF has been undertaken, authorities did not conducted outreach or provided guidance on TF. There were no supervision or monitoring of the NPO sector, there were no obligation for keeping detailed domestic and international transaction records, there were no measures or procedures in place to respond to international requests for information regarding particular NPOs that are suspected of TF or other forms of terrorist support.

Criterion 8.1 **–** a) Art. 9 (e) of the AML/CFT Act, defines *"a corporation"* as a customer being a foundation (as regulated by Act 34/2001 Coll), a non-profit organization providing services of general economic interest (as regulated by Act 213/1997 Coll.), a non-investment fund (as regulated by Act 147/1997 Coll.) and other special-purpose corporations irrespective of their legal personality which manage and distribute funds. The NRA provides general information on the overall level of risk to TF abuse the NPOs face in Slovakia, and give some examples of activities or characteristics, which are likely to carry a higher risk of TF abuse. However, the country did not identify the subset of NPOs which would fall within FATF definition, and the sub-categories which are at risk of TF abuse.

b) According to the NRA, in the period under review (2011-2015), there were no cases where NPOs were used or misused for ML or TF. However, this is a blunt finding of the report not an analysis of the nature of (potential) threats posed by terrorist entities to the NPOs which are at risk. Nonetheless, it must be noted that ways of potential misuse of NPOs for the financing of terrorism are listed on the FIU's website.

c) Slovakia did not make a formal review of the adequacy of measures, including laws and regulations that relate to the subset of NPO sector that may be abused for terrorism financing support. Nevertheless, on a positive note the authorities maintained that in 2019, a new Register of Non-Governmental Non-Profit Organizations was created [63](through the Act No. 346/2018 Coll.). The register is expected to be operational by 1 January 2021 and will include data on the beneficial users of NPOs.

d) There is no specific requirement to periodically re-assess the NPO sector. The only provision in this respect refers to the NRA which shall be updated in particular if there are developments of ML/TF risks and in order to keep it in line with the activity of European Union bodies.

Criterion 8.2 **–** a) The SR has clear legislative rules to promote accountability, integrity and public confidence in the administration and management of NPOs, in particular through specific laws regulating the various legal forms of NPOs, where all relevant data on bookkeeping (single-entry or double-entry accounting) are presented in annual reports, in the register of financial statements, in tax returns, in the register of BOs, while meeting the conditions for applying for a share tax. In the area of transparency of NPOs and their publicly available information, legislative changes were

[63] Non-Governmental Non-Profit Organizations include also foundations, non-profit organizations providing generally useful services, non-investment funds

performed in the SR. The efficiency of the use of public funds is closely related to the record of non-governmental non-profit organizations. The largest organizations in the NPOs sector in terms of financial volume are foundations[64], which are also the most controlled and regulated by legislation (Act no. 34/2002 Coll. on Foundations and on Amendments to the Civil Code). Obligations of foundations related to funding control include: the obligation to prepare financial statements and the annual report, the obligation to have the financial statements and the annual report audited by an auditor, the obligation to publish the annual report and deposit it in the register of financial statements, obligation to file a tax return if it has revenue subject to tax (Art. 34 and 35 of the Act no. 34/2002 Coll.).

b) No systematic and specific outreach to the NPO sector or the donor community on FT issues has been conducted. The authorities asserted that the NPOs are notified by the FSJ of possible misuse of terrorist financing in the context of AML/CFT controls that FIU performs in this sector with four such inspections reported in the period under review. In the course of a meeting between the FIU with the Vice-President of the Government Council for Non-Governmental Non-Profit (March 2019), a procedure was agreed to raise and deepen NPOs awareness on potential vulnerabilities of TF abuse and terrorist financing risks, but no such actions have been reported by the time of the on-site visit.

c) No best practices have been developed in cooperation with NPOs to protect them from FT abuse. The FIU website provides information for NPOs to help them in reducing their vulnerability to potential terrorist financing abuse.

d) Foundations are obliged to deposit funds that are part of the foundation assets, to an account at a bank or a branch of foreign bank. Apart from that, there are no provisions or guidelines encouraging NPOs to conduct transactions via regulated financial channels except publicly available information on the NBS's website with the recommendation to not enter into business relationships with *"problematic"* entities and check the authorization of individual financial market entities on the NBS website.

Criterion 8.3 – Slovakia does not apply a risk-based approach in supervision but authorities report a number of measures applied to all main types of NPOs according to AML/CFT Act or according to sectorial regulation (*i.e.* Act 34/2002 on Foundations, Act 213/1997 on Non-Profit Organizations Providing Public Benefit Services and Act 147/1997 on non-investment funds).

For the purposes of the AML/CFT Act, a foundation, a non-profit organization providing services of general interest, and a non-investment fund are obliged to carry out the identification of the donor and the identification of the natural person or legal entity whose property association has provided funds under Art. 25 of the AML/CFT Act if the value of the donation or the amount of provided funds reaches at least EUR1,000.

The annual reports of the Foundation, a non-profit organization providing services of general interest and a non-investment fund shall be filed in the Register of Financial Statements. All of those shall keep accounts and shall keep accounting records (including annual reports) for the ten years following the year to which they relate (Art. 35(3) of Act 431/2002 on Accounting). On the basis of that document retention, the competent authorities may, if necessary, subsequently verify transactions in order to establish whether the funds have been received and spent in a manner consistent with the purpose and objectives of foundations, non-profit organizations and non-investment funds.

[64] This statement is provided by the Pontis Foundation and available on its website.

The authorities report that in the context of the its rights and obligations, the MoI may impose fines on foundations for failure to submit an annual report.

Criterion 8.4 – a) The authorities stated that the NPOs sector is monitored according to the annual controls plan, used by the FIU when carrying out controls at entities that show the signs of risk. The FIU has implemented a risk-oriented approach to carrying out controls, as referred to in Article 2.1 of the Order of FIU Director no. 126/2018 and in the Methodological Guidelines on the Procedure for Controlling the Compliance of Obligations of Obliged Persons Pursuant to the AML Act by Police Officers of the Obligation of Controlled Persons of FIU no. 34/2018. No other forms of monitoring related to NPO sector by other authorities is in place.

b) The FIU is entitled to conduct controls on NPOs for the purpose of identification of the BO and verification of the veracity and correctness of data about the BO, for the purpose of identifying persons (donors and recipients of donations worth more than EUR 1,000) or for the purpose of checking disposal of property (Art. 25 of the AML/CFT Act). For the non-performance of these obligations, the FIU may impose fines of up to EUR 200,000. (Art. 33 (3) AML/CFT Act). If a foundation fails to perform the obligation to deposit an annual report in the public part of the register of financial statements, the Ministry of the Interior may impose a fine of up to EUR 1,000 (§ 36 of Act 34/2002 Coll. on Foundations). NPOs are legal entities and are subject to Act No. 91/2016 Coll. on Criminal Liability of Legal Entities. As legal entities, NPOs may be criminally prosecuted for committing the offense of ML under § 233 and § 234 of the Criminal Code, and for the offense of terrorist financing under § 419c of the Criminal Code. It results that there is legal base to application of effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs.

Criterion 8.5 – a) Slovakia is effective in NPO related cooperation, coordination and information sharing. If necessary, FIU and LEA are entitled to request information on NPOs from the registry offices (including paper documents such as memorandum of association, statutes, annual reports, etc.). NPOs keep accounts according to Act no. 563/1991 on accounting and are subject to control by the tax authorities. Upon request, the tax authorities provide information to FIU/LEA. According to § 25 para. 2 of the AML Act FIU is authorized to carry out inspections in NPOs also for the purpose of property management. In case of unauthorized disposal of assets in NPOs, the FIU withdraws the LEA information. The FIU shall disseminate the information from the UTRs regarding NPOs to the competent authorities, for example Financial Administration, LEA etc.

b) The National Counter-Terrorism Unit of the National Criminal Agency is a PF unit which has its own investigators and operational search activity specialists who are authorized to examine, detect and investigate suspected terrorist financing. The Slovak authorities indicated that the scope of NPO related crime activities on the territory of the Slovak republic did not sufficiently motivate/justify adoption of specific measures related to additional training or NPO matters schooling for NCTU´s personal. In the absence of such trainings the AT cannot conclude that the National Counter-Terrorism Unit has sufficient investigative expertise and capability to examine NPOs suspected of TF abuse/ TF support

c) Information on the sub-group of organizations that meet the FATF definition of NPOs (mainly non-profit organizations providing services of general interest and foundations) is provided in the register of non-profit organizations and information on foundations kept by the register of foundations. Both these registers are kept by the Ministry of Interior of the Slovak Republic, are available on the Internet and are the source registers for the central register. Hence, this information can be obtained in the course of an investigation.

d) The SIS, FIU and CTU - NAKA are competent to receive and analyse information on any form of TF abuse of NPOs. In addition, on January 1, 2013, the NSAC was established within the SIS organizational structure, with the aim to make cooperation among security forces more effective. The key tasks of NSAC are the preparation of comprehensive analytical assessments of security incidents based on reports and statements received from state authorities, monitoring security situation in open sources and the provision of analytical products on security threats to designated recipients. Although no statistics or examples of NPO abuse information sharing were presented to the AT, from the general scope of NSAC one can deduce that such would fall under the attributions of NSAC.

Criterion 8.6 – The FIU uses the procedures and mechanisms for international cooperation that are provided under the AML/CFT Act, to handle information requests regarding to NPOs. JITs and the Joint Customs Operations – JCO are mechanisms which can be used by the National Counter-Terrorism Unit in the area of the fight against TF under the applicable legislation, including in case a NPO would be involved. JITs and JCOs have not been used in practice, given that no direct activity by terrorist groups has been recorded so far, and no persons or groups have been localized that would prepare to commit a terrorist offense.

Weighting and Conclusion

NPOs sector was assessed as part of the NRA but the authorities have not identified the features and types of NPOs which by virtue of their activities or characteristics, are likely to be at risk of terrorist financing abuse. There was no review of the adequacy of measures, including the subset of NPO sector that may be abused for terrorism financing support. No specific outreach to the NPO sector or the donor community on FT issues has been conducted and no best practices have been developed in cooperation with NPOs to protect them from FT abuse. It seems that there is legal base to application of effective, proportionate and dissuasive sanctions for violations by NPOs or persons acting on behalf of these NPOs. NPO information exchange is done in the usual manner by the FIU. **R.8 is rated PC.**

Recommendation 9 – Financial institution secrecy laws

In the 4th round MER, Slovakia was rated Compliant with the previous R.4. The FATF standards in the area have been amended since then and the new analysis has been undertaken.

Criterion 9.1 – *Access to information by competent authorities* – Art. 18 (Paras.1 & 12) of the AML/CFT Act expressly allows FIs to provide information to FIU without breaching the duty of confidentiality. The sectorial legislation also enables the rest of the competent authorities to access the confidential data and information held by most of the FIs (Act No 483/2001 Coll. on Banks (Article 91(4), 93a(4)), Act No 566/2001 Coll. on Securities and Investment Services (Article 134), Act No 39/2015 Coll. on Insurance (Article 72 (3)), Act No 650/2004 Coll. on Supplementary Pension Savings (Article 34 (14)), Act No 492/2009 Coll. on Payment Services (Article 88 (2)), Act no 186/2009 Coll. on Financial Intermediation and Financial Advisory Services (Article 28 (2), 31(4) (5)), Act no 429/2002 Coll. on Stock Exchange (Article 17(3)), Act no 203/2011 Coll. on the Collective Investment (Article 162(3)), Act no 43/2004 Coll. on Old Age Pension Funds (Article 62(3)). However, the authorities did not provide the relevant disclosure provisions stipulated in the sectorial legislation concerning persons trading in foreign exchange or accounts receivable, and those providing financial leasing

Sharing of information between competent authorities – Art. 26 (3) and 28 of the AML/CFT Act enable FIU to share information with domestic competent authorities and foreign FIUs. The NBS may, to the extent necessary for the performance of its tasks, cooperate and exchange confidential

information with the relevant competent authorities both domestically and internationally at the approval of its Governor by virtue of Article 41 of the Law on National Bank of Slovakia. Law enforcement authorities exchange information both domestically and internationally based on the Article 2 (4) and (6) of the Act No. 46/1993 Coll. on the Slovak Information Service, the Article 34A (3) of the Act No. 171/1993 Coll. on the Police Forces, as well as Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of EU Member States

Sharing of information between FIs - Pursuant to Article 18 (8) of the AML/CFT Act, FIs may exchange information about UTR reporting or other information submitted to FIU, or about measures taken by FIU based on that information with FIs established in the EU member state or third countries with equivalent AML/CFT requirements. However, there are no explicit exemptions from the duty of confidentiality where this is required by R.13, R.16 and R.17, which implies that FI must act within the limits of existing privacy laws that normally require obtaining express written consent from customers to disclose their data.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, the secrecy provisions do not generally inhibit the implementation of the FATF standards. However, the lack of specific exemptions from confidentiality provisions in relation to R.13, R.16 and R.17 affect the overall rating. The authorities also did not provide the relevant disclosure provisions concerning the ability of some FIs to share confidential information with supervisors. **R.9 is rated LC**.

Recommendation 10 – Customer due diligence

In the 4*th* round MER Slovak Republic was rated as LC with the previous R.5. This was largely due to (i) the lack of sufficiently comprehensive requirement for FIs to take reasonable measures to verify the identity of the BO and (ii) the exemption of certain low risk customers from CDD instead of requiring FIs to apply simplified measures. Both the FATF standards and the applicable law were revised since then.

Criterion 10.1 – According to Article 24(2) of the AML/CFT Act, FIs are prohibited from entering into a business relationship or performing a transaction with an anonymous customer. Furthermore, Article 89(2) of the Law on Banks prohibits carrying out transactions of customers on an anonymous basis. Although there is no explicit prohibition on keeping accounts in obviously fictitious names, the AML/CFT Act requires verifying the identity of customers when establishing business relations or carrying out occasional transactions over EUR 1,000.

When CDD is Required

Criterion 10.2 – Art. 10(2) of the AML/CFT Act requires to apply CDD when (i) establishing a business relationship, (ii) carrying out an occasional transaction over EUR 15,000 or in case of a cash transaction, over EUR 10,000, carried out in a single operation or in several operations that appear linked, (iii) when there is a suspicion that the customer is preparing or performing an unusual transaction regardless of its value, or (iv) there are doubts about the veracity or completeness of the previously obtained CDD data. The definition of an unusual transaction (Art. 4) covers suspicions of ML/TF.

Article 10(3) of the AML/CFT Act also requires FIs to identify the customer and verify the customer's identity when carrying out transactions over EUR 1,000. However, this only partially addresses the sub-Criterion (c), which requires the full range of CDD measures (e.g. verifying the

identity of BOs and whether persons purporting to act on behalf of the customer are so authorized) when carrying out occasional wire transfers over EUR 1,000.

Required CDD measures for all customers

Criterion 10.3 –The requirement to identify the customer and verify that customer`s identity is set out in Article 10(1) of the AML/CFT Act. The identity of natural persons is verified on the basis of identity documents and with the physical presence of a customer or by non-face to face interaction using technical means that ensure the same degree of reliability (Art. 8(1)(a)). Legal persons including state authorities, are verified based on the data or documents obtained from official corporate registers or other reliable and independent sources.

Criterion 10.4 – Article 10(7) of the AML/CFT Act stipulate that when carrying out due diligence, the obliged person shall ascertain whether the customer acts in their own name. If the obliged person finds out that the customer does not act in their own name, it shall Articles 7(1)(c) and 8(1)(c) of the AML/CFT Act stipulate the obligation to identify and verify the identity of a person who, on the basis of the power of attorney, acts on behalf of a customer. Particularly, the obliged person shall call upon the customer to prove, through a binding written declaration, the name, surname, personal number or date of birth of the natural person, or the business name, registered office, and identification number of the legal entity, in whose name the transaction is carried out. This information is then to be verified. The obliged person shall follow the same procedure in case that there are doubts whether the customer acts in their own name.

However, these do not amount to requiring FIs in all instances to verify whether persons purporting to act on somebody else's behalf are so authorized and verify the identity of that person and the customer (in case the person is not acting based on the power or attorney).

Criterion 10.5 – Article 10(1)(b) of the AML/CFT Act requires FIs to identify the BO and take adequate measures to verify his/her identity. FIs are also not permitted to solely rely on the data obtained from corporate registries and public authorities. However, this does not amount to the requirement to verify BOs based on reliable source data so that the FI is satisfied that it knows who the BO is. The BO is defined by Article 6a of the AML/CFT Act as the natural person who ultimately owns or controls the legal entity, an entrepreneur natural person or any other natural person in whose favour a transaction/activity is being conducted. This definition however does not cover all instances when a natural person ultimately controls another natural person.

Criterion 10.6 – Article 10(1)(c) of the AML/CFT Act requires FIs to obtain information about the purpose and intended nature of a business relationship. However, there is no requirement to regard to understanding the purpose and intended nature of the business relationship.

Criterion 10.7 – According to Article 10(1)(g) of the AML/CFT Act, FIs must carry out the ongoing monitoring of business relationships, including the scrutiny of transactions undertaken throughout the course of those relationships to ensure that transactions are consistent with their knowledge of the customer and its business and risk profile. FIs must also ensure that CDD documents, data and information are kept updated. However, there is no specific requirement to examine, where necessary, whether transactions of the customer are consistent with the source of funds.

Specific CDD measures required for legal persons and legal arrangements

Criterion 10.8 – Article 10(1)(b) of the AML/CFT Act requires FIs to understand the ownership and control structure of clients (legal entities and trusts) in the process of establishing BOs. There is however no specific obligation to understand the customer's business, although FIs must

examine the consistency of transactions undertaken with the customer's business profile as part of the on-going due diligence.

Criterion 10.9 – The data required to identify legal entities and the sources of verification therein are set out in Articles 7(1)(b) and 8(1)(b) of the AML/CFT Act. Thus, FIs are required to obtain the name of the legal entity and address of its registered office. FIs are also required to identify the natural person authorized to act on behalf of the legal entity. These data must be verified based on the information or documents obtained from the official corporate registry or other reliable and independent sources. In case of corporate registries, the proof of existence (e.g. certificate of incorporation, extract) would normally be obtained; however may also obtain relevant information from other credible sources, which may not contain the information mentioned by authorities. Identifying the natural person authorized to act on behalf of the legal entity also does not amount to obtaining the names of all relevant persons holding the senior management position (e.g. senior managing directors). And finally, FIs are not required to distinguish the address of the registered office of the legal entity from its principal place of business, and if different, obtain the relevant information.

Regarding the registered address – the legal entities have **one r**egistered address/"seat" listed in Commercial register (art. 2/ 3 of the Commercial Code). Natural persons have the "place of business" listed in the Trade register (art. 60/2/d law No.: 455/1991 Coll. on Business). Corporations have "seat" listed in their respective registers, see effectiveness part. (Foundation, non-profit organization non-investment fund – art. 2/ 2 / a), b) a c), and art. 2 / 1 / a) law No.: 346/2018 Coll. on the register, non-governmental organizations. No other residences, seats or addresses are subject to registration.

Criterion 10.10 – BO of the legal person is defined by Article 6a(1)(2) of the AML/CFT Act and includes the natural person(s) who:

(a) ultimately owns or controls the legal entity through direct or indirect ownership or control of at least 25% of shares or voting rights including through bearer shareholdings, or benefits from at least 25% of the economic activity of the business;

(b) is authorized to appoint, otherwise determine the composition of or withdraw the statutory, managing, supervisory or audit bodies, or controls the legal person in any other way;

(c) is the member of top management in case no other person meets the criteria noted above. The member of top management is defined as the member of the statutory body, procurator or manager under the direct authority of the statutory body. Pursuant to Article 6(2) of the AML Law, in case that any person doesn´t meet criteria listed in Article 6(1)(A) of the law, members of top management shall be considered as the BO of the entity; member of top management means a statutory body, a member of the statutory body, procurator and manager under the direct authority of the statutory body. The authorities explained that where several persons act in those capacities, all of them shall be considered as senior managing officials.

Criterion 10.11 – Pursuant to AML/CFT Act (Article 6a(1)) persons that ultimately control the trust are considered as BOs. Specific definition of the BO of the trust is provided under Article 6a(1)(c) of the AML/CFT Act. BO of the trust is the founder (settlor) and the known beneficiary of at least 25% of resources held in trust or where such a beneficiary is yet to be identified, the person(s) who benefits significantly from the activity of a trust. This definition is not in line of the requirements of EC10.11 as it required identification based on a threshold and it does not cover the protector (where applicable. There are no specific requirements concerning beneficiaries

designated by characteristics or class. Moreover, there is no similar definition of BOs is provided for other types of legal arrangements under the AML/CFT Act.

CDD for beneficiaries of life insurance policies

Criterion 10.12 – Beneficiaries of life insurances policies must be identified and verified prior to or at the time of payout, or when the beneficiary intends to exercise the rights vested under the policy. There is however no specific requirement to gather the relevant information in relation to beneficiaries designated by characteristics or class to satisfy the FI that it will be able to establish the identity of the beneficiary at the time of the pay-out. The authorities did not provide information about other investment-related insurance policies and the applicable requirements.

Criterion 10.13 – There is no requirement to include the beneficiary of a life insurance policy as a relevant risk factor when determining whether to apply enhanced CDD.

Timing of Verification

Criterion 10.14 – Pursuant to Article 8(2) of the AML/CFT Act, FIs are required to verify the identity of the customer and BO before establishing a business relationship or carrying out a transaction. The verification may be completed after establishing the business relations provided that it is necessary to not interrupt the normal conduct of business, ML/TF risks are low and the verification is finalized without undue delay (Art. 8(3)).

Criterion 10.15 – The AML/CFT Act provides for the general requirement for FIs to put in place the relevant measures to manage ML/TF risks (Art. 20(2)(c)) and verification may be completed after the establishment of the business relationship only if the ML/TF risks are low. In case of bank accounts, including accounts that allow transactions in transferrable securities, only crediting operations are allowed before the customer and BO are duly verified.

Existing Customers

Criterion 10.16 – The transitional provisions of the AML/CFT Act (Art. 36(1)) required obliged entities to conduct CDD (according to new national requirements), depending on the risk, in relation to existing customers within a year from when the law entered into force. However, there are no provisions that would require FIs to apply CDD to existing customers depending on the materiality and, when determining appropriate times, to also take into account whether and when CDD measures have previously been undertaken and the adequacy of the data obtained.

Risk-Based Approach

Criterion 10.17 – Article 12(1) of the AML/CFT Act requires FIs to apply enhanced CDD measures based on a risk assessment in every case where higher ML/TF risks have been identified. It further stipulates some higher ML/TF situations where the enhanced CDD is mandatory: for example, (i) cross-border correspondent banking relationships, (ii) transactions or business relations with PEPs and (iii) with persons established in high-risk countries as designated by the European Commission, (iv) non-face to face verification of customers. At the same time, this list is non-exhaustive and the decision whether or not to conduct enhanced CDD should be based on the initial risk assessment, the criteria of which are broadly described in the annex of the AML/CFT Act. The AML/CFT Act defines the enhanced CDD as the application of additional CDD measures depending on the ML/TF risk.

Criterion 10.18 – Article 11(1)(2) of the AML/CFT Act provides for the possibility of applying simplified CDD measures in certain low risk scenarios, which are not justified by the findings of the NRA. The authorities did not provide any other relevant analysis of risks that underpins those

scenarios. The FIs are prohibited from performing simplified CDD measures when there is suspicion of an unusual transaction (Art.11 (3)).

Failure to Satisfactorily complete CDD

Criterion 10.19 **–** Article 15 of the AML/CFT Act stipulates that FIs are required to refuse establishing a business relationship or performing a transaction, and to terminate a business relationship if they cannot identify and verify customers or BOs, ascertain their PEP status or obtain information about the purpose and intended nature of a business relationship. However, no such requirement exists where FIs cannot perform other required CDD measures such as conducting ongoing due diligence.

According to Article 17(1) of the AML/CFT Act, FIs are required to report an unusual transaction to FIU without undue delay. Article 4(2)(c) defines unusual transactions as including instances when the customers refuse to identify themselves or provide the relevant CDD data. This reporting obligation does not extend to all circumstances which a financial institution is unable to comply with the relevant CDD measures*.*

CDD and Tipping-off

Criterion 10.20 **–** The AML/CFT Act does not permit FIs to refrain from pursuing the CDD process in cases where it is reasonably believed that the performance of CDD measures will tip-off the customer.

Weighting and Conclusion

The Slovak Republic has many of the necessary CDD requirements in place. However, there are a considerable number of gaps which undermine the overall effectiveness of the CDD framework, such as deficiencies with regard to conducting full range of CDD measures when carrying out occasional wire transfers over threshold., the definition and verification of BOs understanding the purpose and intended nature of the business relationship, no specific requirement to examine, where necessary, whether transactions of the customer are consistent with the source of funds and obligation to understand the customer's business profile. Besides, deficiencies have also been identified in the identification and verification measures for legal persons and legal arrangements (including identification and verification of Bos of legal arrangements). Deficiencies have been identified in relation of CDD for beneficiaries of life insurance policies. There are no provisions that would require FIs to apply CDD to existing customers depending on the materiality. Low risk scenarios for applying simplified CDD are not justified by the findings of any NRA. There is no requirement to refuse to perform the transaction or to terminate the business relationship where FIs cannot perform some CDD measures such as conducting ongoing due diligence. The reporting obligation does not broadly extent to the circumstance when a financial institution is unable to comply with the relevant CDD measures. There is no explicit provision in case of risk of tipping-off the customer followed by submission of a UTR. **R.10 is rated PC.**

Recommendation 11 – Record-keeping

In the 4th round MER, Slovakia was rated as LC with the previous R.10. There was no explicit requirement for FIs to maintain the account files and business correspondence. The domestic legislation also lacked the clear requirement of making the customer and transaction records and information available to competent authorities in a timely manner. The applicable standards were revised since then and the new analysis has been undertaken.

Criterion 11.1 **–** Article 19(2)(b) of the AML/CFT Act requires FIs to maintain all the data and written documents concerning a transaction for 5 years after its completion. The definition of

"transaction" pursuant to Article 9(g) of the AML/CFT Act is sufficiently broad to cover both domestic and international transactions.

Criterion 11.2 – FIs are required to keep all the data and written documents obtained through CDD, EDD and SDD measures, as well as the results of analyses of unusual transactions for 5 years after the termination of the business relationship according to Article 19(2)(a) of the AML/CFT Act. For occasional customers only data related to the transaction is kept (Art. 19(2)(b). The record-keeping requirements do not cover the business correspondence and account files that are not always part of the CDD data and would normally encompass all supporting documents, data and information in respect of an account. Moreover, it does not extend to the results of analyses undertaken by FIs in contexts other than identifying unusual transactions.

Criterion 11.3 – According to Article 19(5) of the AML/CFT Act, FIs are obliged to retain the copies of documents in a way that makes them legible, while the image of the natural person must be kept sufficiently clear to enable the verification of appearance. The requirements to keep transaction records that are sufficient to permit the reconstruction of individual transactions so as to provide, if necessary, evidence for criminal prosecution is met.

Criterion 11.4 – Article 21(1)(2) of the AML/CFT Act requires FIs to make all the data and written documents on business relationships and transactions available upon the request of and in the timeframe set by the FIU. The requirement to submit relevant information to competent authorities is also addressed under separate legal provisions which allow authorities to request information from FIs[65]. FIs are also specifically required to put in place appropriate systems to ensure the swift submission of the requested data and documents.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, the requirement to keep the records obtained through CDD measures for 5 years does not seem to apply to occasional customers. The record-keeping requirements also do not cover the business correspondence and account files, and the results of analyses undertaken outside the context of identifying unusual transactions. **R.11 is rated LC.**

Recommendation 12 – Politically exposed persons

In the 4th round MER, Slovakia was rated as PC with the previous R.6. There was no requirement to verify if the BO was a PEP or to obtain the approval of senior management for continuing the business relationship where the customer was subsequently found to be a PEP. The definition of foreign PEPs also excluded the residents of Slovak Republic and did not cover all individuals entrusted with prominent public functions.

Criterion 12.1 – The definition of PEPs is provided by Art. 6 of the AML/CFT Act and is in full compliance with the FATF standards.

(a) Article 10 (1) (d) of the AML/CFT Act requires FIs to ascertain whether the customer or the BO is a PEP as part of CDD measures. There is no specific requirement to put in place the risk

[65] Act No 483/2001 Coll. on Banks (Article 91(4), 93a(4)), Act No 566/2001 Coll. on Securities and Investment Services (Article 134), Act No 39/2015 Coll. on Insurance (Article 72 (3)), Act No 650/2004 Coll. on Supplementary Pension Savings (Article 34 (14)), Act No 492/2009 Coll. on Payment Services (Article 88 (2)), Act no 186/2009 Coll. on Financial Intermediation and Financial Advisory Services (Article 28 (2), 31(4) (5)), Act no 429/2002 Coll. on Stock Exchange (Article 17(3)), Act no 203/2011 Coll. on the Collective Investment (Article 162(3)), Act no 43/2004 Coll. on Old Age Pension Funds (Article 62(3)).

management systems for identifying PEPs, although the extent of CDD measures should be determined based on ML/TF risk (Art. 10(4)).

(b) Article 12 (2) (c) (1) of the AML Act requires FIs to obtain the approval from the management board or a designated person before establishing or continuing a business relationship. The designated person must either be a member of the management board of an FI or a manager who has direct communication with the statutory and supervisory boards, and can access all required information and documents. The latter does not seem to be equivalent to senior manager. (c) Article 12 (2) (c) (2) of the AML/CFT Act requires FIs to establish the source of wealth and source of funds involved in business relationships and transactions with PEPs. Thus, it appears that FIs are not required to take reasonable measures to establish the origin of the entire body of wealth (total assets) of customers and BOs identified as PEPs.

(d) Article 12 (2) (c) (3) of the AML/CFT Act requires FIs to apply enhanced on-going monitoring of the business relationship with PEPs.

Article 12 (3) of the AML/CFT Act provides that FIs must continue applying the measures noted above in relation to persons who are no longer entrusted with a prominent public function for at least 12 months and until such time as the person poses no PEP-specific ML/TF risk based on the risk assessment of an FI. This approach is in line with the FATF Guidance on PEPs, which requires handling of a customer who is no longer entrusted with a prominent public function based on an assessment of ML/TF risks.

Criterion 12.2 – The AML/CFT Act does not distinguish between the domestic and foreign PEPs, and those who are members of the management bodies of the EU institutions and international organizations. Thus, FIs must apply measures noted in c.12.1 to all types of PEPs.

Criterion 12.3 – The definition of family members of PEPs is provided by the Art. 6 (3) of the AML/CFT Act and includes spouses, parents, children and their spouses and those equivalent to spouses. The definition of family members however does not include siblings of PEPs, which is part of the minimum standard provided by the FATF Guidance on PEPs. Persons considered as close associates of PEPs are limited to those who have joint beneficial ownership of the FI's customer, run business together with PEPs or have beneficial ownership of the FI's customer set up in favour of a PEP. This approach is more restrictive than is called for by the FATF Guidance on PEPs.

Criterion 12.4 – FIs providing life insurance policies are not required to take reasonable measures to determine whether the beneficiaries, and where required, the BO of the beneficiary, are PEPs. Other elements of c.12.4 are also not fulfilled, although the senior management must be informed whenever policy proceeds are paid out as part of the business relationship with PEPs.

Weighting and Conclusion

FIs are not specifically required to put in place risk management systems for identifying PEPs. They are also not required to take reasonable measures to establish the origin of the entire body of wealth of PEPs. Definitions of family members and close associates of PEPs are restrictive, while none of the elements of c.12.4 are met. **R.12 is rated PC**.

Recommendation 13 – Correspondent banking

In the 4th round MER, Slovak Republic was rated as LC with the previous R.7. the requirements concerning the cross-border correspondent relationship applied to only non-EU/EEA countries. FIs engaged in correspondent relationships with third country FIs were also not required to document the responsibilities of each institution, although this was common in practice.

Criterion 13.1 – The correspondent relationship is defined by the AML/CFT Act (Art. 9(k)). Prior to establishing a cross-border correspondent relationship (but with only those FIs outside EEA area), FIs are required to:

(a) Gather information about the respondent institution to fully understand the nature of its business and determine from publicly available sources its reputation and the quality of supervision applied therein (Art. 12 (2)(b)(1), the AML/CFT Act). However, there are not being gathered information with regard to whether (and when) the respondent institution has been subject to a ML/TF investigation or regulatory action. While correspondent banks are required to determine the quality of supervision of a respondent bank, they are not required to determine if the respondent has been subject to a ML/FT investigation or regulatory action.

(b) Assess the respondent institution's AML/CFT controls (Art. 12 (2)(b)(2), the AML/CFT Act).

(c) Obtain the senior management (statutory body or the designated manager in direct communication with the statutory body and with access to the information and documents obtained from the obliged person during performing CDD) approval for establishing a new correspondent relationship (Art. 12(2)(b)(3), the AML/CFT Act);

(d) Document the responsibilities of each institution (Art. 12(2)(b)(4), the AML/CFT Act). However, FIs are not specifically required to make sure that the outcome of this exercise is a *clear understanding* of those responsibilities. The correspondent institution should clearly understand how the respondent institution will be offering services available through the correspondent banking relationship to its customers and assess the nature and level of risk associated with offering arrangements. The documentation should be an action based on precise information/documents, other than the enhanced due diligence measures applied in respect to cross border correspondent banking, that will provide a clear understanding of the AML/CFT responsibilities of each institution.

Criterion 13.2 – Article 12(2)(b)(5) of the AML/CFT Act requires FIs, with regard to payable-through accounts, to ensure that the respondent institution performed CDD obligations in relation to the customer that has direct access to the correspondent account and is able to provide relevant information upon request. However, this requirement applies to only non-EU/EEA countries.

Criterion 13.3 – Art. 24 of the AML/CFT Act stipulates that FIs must not enter into or continue a correspondent relationship with a shell bank or a bank that is known to have entered into a correspondent relationship with a shell bank.

Weighting and Conclusion

The correspondent banking requirements (except for those related to shell banks) do not apply to EU/EEA countries. Correspondent banks are not required to determine if the respondent has been subject to a ML/FT investigation or regulatory action. FIs are also not *specifically* required to assess the *quality* of respondent FIs' AML/CFT controls, *clearly understand* the AML/CFT responsibilities of each institution. **R.13 is rated PC**.

Recommendation 14 – Money or value transfer services

In the 4th round MER, Slovak Republic was not assessed in relation to the previous SR VI. In the 3rd round assessment, the AT found that there was no legal provision determining what information about transactions must be recorded by MVTS providers. The applicable FATF standards were significantly revised since then and the new analysis has been undertaken.

Criterion 14.1 – The Law on Payment Services (No 492/2009) requires all MVTS providers (banks, foreign banks or a branch of a foreign bank, a post office institution, payment and e-money institutions), which can only be legal persons, to obtain the relevant license/authorization from the NBS before the provision of services (Art. 2(3)).

Criterion 14.2 – The NBS is authorised to exercise supervision over the MVTS providers, monitor their online activity and collect information from other external sources to guard against the provision of those payment services that have not been authorized. Where such instances are identified, the Law on Payment Services allows the NBS to apply a variety of sanctions including the imposition of a fine up to EUR 300,000 (or in case of repeated or severe violations, up to EUR 600,000), suspension of activities and partial or full withdrawal of the authorization (Art. 78(2)).

The NBS is also authorized to request and obtain the relevant information from any person suspected of providing unauthorized payment services and to also verify that information at the place of business under the Law on Payment Services (Art. 78(9)). Where the NBS concludes that unauthorized payment services have indeed been provided, it shall report to LEAs and can impose sanctions similar to those noted above depending on the gravity, scope, duration, impact and character of the violation (Art. 78(10)). The authorities have not provided information about the modalities of identifying the provision of unauthorized payment services by persons other than authorized institutions or the applicable criminal sanctions.

***Criterion* 14.3 –** MVTS providers are obliged entities under the AML/CFT Act and are therefore subject to monitoring for compliance by the NBS (See analysis in R.26).

Criterion 14.4 – According to Article 75 of the Law on Payment Services, a payment institution seeking to provide services via an agent must notify the NBS about the intention and submit the relevant information about the agent including the description of its AML/CFT controls. Only once registered (put on the list of agents) by the NBS, may the agents start providing services on behalf of a payment institution. Agents registered in other EU member states may provide payment services in Slovak Republic if the NBS receives the relevant notification from supervisors in those states under Article 79(5). The up-to-date list of agents of payment institutions is published by the NBS on its website (Art. 74(3)).

Criterion 14.5 – There is no requirement for payment institutions to include their agents in AML/CFT programs and monitor compliance therein. However, agents of payment institutions i.e. payment service agents are obliged entities under the AML/CFT Act. They are required to put in place their own AML/CFT programs (Art. 20) and are being supervised for compliance with the relevant AML/CFT requirements (Art. 29).

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, no information was provided on the ways of identifying the provision of unauthorized payment services by persons other than authorized institutions by the NBS or other competent authority. **R.14 is rated LC.**

Recommendation 15 – New technologies[66]

[66] The FATF revised R.15 in October 2018 and its interpretive note in June 2019 to require countries to apply preventive and other measures to virtual asset service providers and virtual asset activity. This evaluation does not assess Slovakia's compliance with revised R.15 because, at the time of the on-site visit, the FATF had not yet revised its assessment Methodology. Slovakia will be assessed for technical compliance with revised R.15 in due course, in the context of its mutual evaluation follow-up process.

In the 4th round MER, Slovakia was rated as PC with the previous R.8. The main deficiency was related to the effectiveness of ensuring compliance with legal requirements, namely the lack of guidance on dealing with risks arising from new technologies. The FATF standards were revised since then by incorporating requirements on a non-face to face business in R.10, and putting more emphasis on the identification and mitigation of risks arising from new products and technologies in R.15.

Criterion 15.1 – Art. 26a of the AML/CFT Act requires FIU to assess national ML/TF risks and to take into account a number of risk factors provided in Annex No. 2, which include new products, business practices and delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Similarly, Article 20a of the Law requires FIs to assess their business-specific ML/TF risks taking into account at least the very same risk factors. Article 14(2)(b) further stipulates that FIs must pay special attention to ML/TF risks related to new technologies that favour anonymity.

Criterion 15.2 – Art. 20(1) of the AML/CFT Act requires FIs to update their AML/CFT programs accordingly before starting the provision of new products that increase their ML/TF risk exposure. Hence, FIs are effectively required to assess ML/TF risks before the new products are launched. However, no such requirement exists in relation to new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products.

Art. 20a(2) of the AML/CFT Act requires FIs to have in place measures aimed at managing risks identified as part of their risk assessments, while Art. 14(2)(b) specifically requires undertaking proper measures to prevent the misuse of new technologies that favour anonymity. Art. 8(1)(a) allows for non-face to face verification of natural persons by FIs. However, the technology used in the process should ensure that the verification is carried out at the same level of reliability as during the physical presence of a customer.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, FIs are not required to conduct risk assessments *prior* to the launch or use of new business practices and the new or developing technologies. **R.15 is rated LC**.

Recommendation 16 – Wire transfers

In the 4th round MER, Slovak Republic was rated Compliant with the previous SR VII.

Ordering FIs

Criterion 16.1 – The EU Regulation 2015/847 on information accompanying transfers of funds is directly applicable to all EU member states. With respect to R.16, domestic wire transfers refer to transfers entirely within the borders of the EU, while cross-border wire transfers represent transfers made to/from third countries.

a) All cross-border wire transfers exceeding EUR1,000 should be accompanied by the following information on the payer i.e. the originator: the name of the payer; the payer's payment account number; the payer's address, official personal document number, customer identification number or date and place of birth. In case of a wire transfer not made from a payment account, the PSP of the payer shall ensure that the transfer is accompanied by a unique transaction identifier (Art. 4). The PSP of the payer has the obligation to always verify the accuracy of the payer information on the basis of documents, data or information obtained from a reliable and independent source before transferring funds.

b) All cross-border wire transfers exceeding EUR1,000 shall be accompanied by the following information on the payee i.e. beneficiary: the name of the payee; the payee's payment account number. In case of a wire transfer not made to a payment account, the PSP of the payer shall ensure that the transfer is accompanied by a unique transaction identifier (Art. 4).

Criterion 16.2 – In case of a batch file cross-border transfer from a single payer, the batch file must contain the required and verified information on the payer and the required information on the payee, while individual transfers should carry the payment account number of the payer or the unique transaction identifier (Art. 6(1)).

Criterion 16.3 – If a wire transfer does not exceed EUR1,000 (and does not appear to be linked to other wire transfers which together exceed EUR1,000), it must be accompanied with the names of the payer and the payee, their account numbers, or were applicable – the unique transaction identifier (Art. 6(2)).

Criterion 16.4 – In case of wire transfers not exceeding EUR 1,000, the payer's PSP need not verify the information on the payer unless there are reasonable grounds for suspecting ML/TF (Art. 6(2)). Additionally, Article 10(2)(c) of the AML/CFT Act stipulates that suspicious transactions, irrespective of threshold, must always be subject to CDD measures.

Criterion 16.5&16.6 – Domestic wire transfers must be accompanied by at least the payment account number of both the payer and the payee or the unique transaction identifier (Art. 5(1)). The PSP of the payer shall, within 3 working days of receiving a request for information from the PSP of the payee or from the intermediary PSP, make available the requested information. PSPs are also required to respond fully and without delay to enquiries from competent AML/CFT authorities (Art.14).

Criterion 16.7 – The required information on the payer and the payee must be retained by the PSP of the payer for 5 years (Art.16).

Criterion 16.8 – The PSP of the payer is prohibited from executing a wire transfer without complying with the requirements of c.16.1-c.16.7 (Art.4(6)).

Intermediary FIs

Criterion 16.9 – The intermediary PSPs are required to ensure that the information on the payer and the payee, that accompanies a wire transfer, is retained with it (Art.10).

Criterion 16.10 – There is no exemption provided by the EU Regulation 2015/847 concerning technical limitations that prevent the appropriate implementation of the requirements on domestic wire transfers.

Criterion 16.11 – The intermediary PSP is required to implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the information on the payer or the payee is missing in a cross-border wire transfer.

Criterion 16.12 – The intermediary PSP is required to have effective risk-based procedures for determining whether to execute, reject or suspend a wire transfer lacking the required information on the payer or the payee, and for taking the appropriate follow-up action (Art. 12). If the PSP has not been provided with the required payer or payee data, it shall reject the transfer or ask for the required information on the payer and the payee before or after the transmission of the wire transfer, on a risk-sensitive basis.

Beneficiary FIs

Criterion 16.13 – The PSP of the payee shall implement effective procedures, including, where appropriate, ex-post monitoring or real-time monitoring, in order to detect whether the information on the payer or the payee is missing in a cross-border wire transfer (Art.7(2)).

Criterion 16.14 – In case of wire transfers exceeding EUR 1,000, the PSP of the payee must verify the accuracy of the information on the payee on the basis of documents, data or information obtained from a reliable and independent source before crediting the payee's payment account or making funds otherwise available to the payee. The information on the payee must be retained by the PSP of the payee for 5 years (Art.16).

Criterion 16.15 – The PSP of the payee must implement the risk-based procedures to determine whether to execute, reject or suspend a wire transfer lacking the required information on the payer and payee, and for taking the appropriate follow-up action. (Art.8).

MVTS operators

Criterion 16.16 – The EU Regulation 2015/847 is binding for all MVTS providers and, according to Article 2, applies to wire transfers, in any currency, which are sent or received by a PSP of the payer or the payee, or an intermediary PSP established in the EU. MVTS providers operating in third countries (through a branch or subsidiaries) are also required to take measure equivalent to performing customer due diligence and record keeping (art. 5, 10, 11, 12, 19 and 21 (4) (5) of the AML Law).

Criterion 16.17 – The situation where one MVTS provider controls both the payer's and the payee's side of a wire transfer is not specifically addressed by the EU Regulation 2015/847. However, MVTS providers and their agents are obliged entities under the AML/CFT Act and must take into account all the available information to identify suspicious transactions and file those to FIU. Nevertheless, there is no requirement to file a UTR in the country affected by the suspicious wire transfer and to make relevant transaction information available to the FIU.

Implementation of Targeted Financial Sanctions

Criterion 16.18 – FIs have the obligation to take freezing action and refuse transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions in relation to all transactions, including wire transfers.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, there is no requirement under the AML/CFT Act to file a UTR in the country affected by the suspicious wire transfer and to make relevant transaction information available to the FIU. **R.16 is rated LC**.

Recommendation 17 – Reliance on third parties

In the 4th round MER Slovak Republic was rated as LC with the previous R 9. Investment service providers, unlike other FIs, could rely on third parties to perform CDD measures, but the AT was not sufficiently informed about their compliance with the relevant requirements. The FATF standards were revised since then to stress the importance of a third-party country risk. The applicable legal provisions also changed and the new analysis has been undertaken.

Criterion 17.1 – According to Article 13(1) of the AML/CFT Act, FIs may rely on other FIs located in jurisdictions, which impose the equivalent CDD and record-keeping requirements, to perform CDD measures concerning the identification and verification of customers and BOs, and

understanding the purpose and intended nature of business relationships. The responsibility for applying the required CDD measures remains with the relying FI (Art. 13(3)).

(a) & (b) The AML/CFT Act (Art. 13(2)) requires the immediate provision by the third party of both the data obtained through CDD measures and the copies of relevant documents to the relying FI.

(c) The AML/CFT Act (Art. 13(1)) stipulates that the third party should be supervised for compliance with CDD and record-keeping requirements in line with the relevant EU legislation, however this does not necessarily amount to compliance with the requirements set out in R.10 to R.12 and R.18. There is however no specific legal provision stating that the third party must have measures in place for compliance with those requirements.

Criterion 17.2 – FIs are not allowed to rely on third parties from high-risk jurisdictions as identified by the EU under the AML/CFT Act (Art. 13(4)). However, the relevant EU regulation (2016/1675) on high-risk jurisdictions applies only to non-EU/EEA states (see the analysis in R.19) and it is not equivalent to the obligation to have regard to information on the level of country risk.

Criterion 17.3 – There are no specific legal provisions applicable to third party reliance within the same financial group and thus general requirements apply.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, FIs are not specifically required to satisfy themselves that third parties have measures in place to comply with the relevant CDD and record-keeping requirements, although they must be supervised for compliance therein. FIs are prohibited to rely on third parties from countries placed on the EU list of high-risk jurisdictions, which only includes non-EU/EEA states and it is not equivalent to the obligation to have regard to information on the level of country risk. **R.17 is rated LC.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In the 4th round MER, Slovak Republic was rated as PC with the previous R.15 and R.22. There were no specific requirement that the AML/CFT compliance officer be placed on a managerial level and have timely access to the required data. There was also no legal provision requiring FIs to adopt screening procedures or enable the AML/CFT compliance officer to act independently and report to senior management. FIs were required to ensure that their foreign branches and majority-owned subsidiaries were applying FATF standards, but only in relation to non-EU/EEA countries.

Criterion 18.1 – The AML/CFT Act requires FIs to put in place AML/CFT programs (Art. 20 (1)) taking into consideration its own organisational structure and activity and must be approved by the FI's statutory body (Art. 20a(2)). There is however no specific requirement to also take into account the size of the business when designing those programs.

(a) Article 20(2)(h) of the AML/CFT Act requires the designation of the FI's statutory body or its member or a manager in direct communication with the statutory and supervisory bodies in charge of AML/CFT compliance. The AML/CFT compliance officer/body should have access to all required CDD information and documents. Nevertheless, there is no requirements that the compliance officer should be at management level.

(b) There is no legal provision requiring FIs to screen their employees in order to ensure high standards when hiring.

(c) The AML/CFT Act requires FIs to ensure professional training of employees in the AML/CFT programme (Art. 20(3)) and the identification of unusual transactions (Art. 20(3)). Such trainings must be held annually and also before assigning a new employee to the job**.**

(d) There is no specific requirement to put in place an independent audit function for the purpose of testing the AML/CFT system. The general requirement to carry out internal audit of management and controls systems is present in the sectorial legislation all FIs.

Criterion 18.2 – The AML/CFT Act requires FIs to apply group-wide AML/CFT programs to their branches and majority-owned subsidiaries in third countries (Art. 20a(3)). This requirement however does not extend to branches and subsidiaries in EU member states.

(a) The group-wide AML/CFT programs must include procedures for information-sharing within the group under the AML/CFT Act (Art. 20a(3)). This requirement however does not extend to branches and subsidiaries in EU member states.

(b) There is no specific requirement that the group-wide AML/CFT programs provide for the collection of the relevant customer, account and transaction data at the group-level functions, or the dissemination of those data to members of the group for risk management purposes.

(c) There is no specific requirement to include adequate safeguards on confidentiality (except for personal data-protection) and prevention of tipping-off in the group-wide AML/CFT programs.

Criterion 18.3 – Article 21(5) of the AML/CFT Act requires FIs to ensure that their branches and majority-owned subsidiaries in third countries take AML/CFT measures in line with the domestic and EU legislation. If third countries do not permit the implementation of those measures, FIs must inform FIU and adopt additional AML/CFT measures. However, these requirements do not extend to branches and subsidiaries in EU member states. Article 21(4) of the AML/CFT Act stipulates that when branches and other organizational units are located in EU members states, FIs must ensure that the AML/CFT legislation of the host country is followed. Thus, all EU countries are presumed to have adequate AML/CFT measures.

Weighting and Conclusion

FIs are not specifically required to take into account the size of the business when designing AML/CFT programs or include employee screening procedures and independent audit function in those programs. Moreover, FIs are required to apply group-wide AML/CFT programs, and ensure the implementation of FATF standards, or management of risks when implementation of FATF standards is not allowed by host countries, only in relation to branches and subsidiaries outside the EEA area. There are also deficiencies concerning the procedures for information-exchange and protection of confidentiality in the group-wide AML/CFT programs. **R.18 is rated PC**.

Recommendation 19 – Higher-risk countries

In the 4th round MER, Slovakia was rated as NC with the former R.21. There were insufficient measures in place to ensure that FIs were advised of weaknesses in AML/CFT systems of other countries. No specific requirement existed to examine the background and purpose of unusual transactions, and to document findings therein in writing. The competent authorities were also not authorized to apply any countermeasures.

Criterion 19.1 – Art. 12(1) of the AML/CFT Act obliges FIs to perform enhanced CDD to a transaction or business relationship with the person *established* in a high-risk jurisdiction with strategic deficiencies as identified by the EU. This falls short of the FATF standard. Although the current EU list includes all those jurisdictions for which enhanced CDD measures are called for by

the FATF, the relevant EU regulation (2016/1675) applies to only non-EU/EEA states. Moreover, it is unclear whether enhanced CDD measures must be applied to natural persons who reside in the high-risk jurisdiction or legal persons that primarily operate, but are not formally incorporated in such a jurisdiction.

Criterion 19.2 – The countermeasures that can be applied by Slovakia are limited to enhanced CDD measures. Other countermeasures cannot be applied either independently or when this is called for by the FATF, because it is constrained with the list of jurisdictions identified as high risk by the EU.

Criterion 19.3 – FIU is only publishing the decisions taken by the European Commission that identify high-risk jurisdictions with strategic deficiencies.

Weighting and Conclusion

There are moderate shortcomings to R.19. Enhanced CDD measures can only be applied to high-risk countries that are not part of the EEA area. Slovakia is not able to apply countermeasures either independently or when called for by the FATF. Only decisions of the European Commission identifying high-risk jurisdictions are published by FIU. **R.19 is rated PC.**

Recommendation 20 – Reporting of suspicious transaction

In the 4th round of evaluations Slovakia was rated PC with the former Recommendation 13 and SR. IV. The main reasons were that no clear reporting obligation was covering funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations, deficiencies in the definition of terrorist financing in the AML/CFT Act could had an impact on the reporting of suspicious transactions, there were no specific guidance or indicators for recognising suspicious transactions needed for all reporting institutions. Also, there were effectiveness issues due to the fact that only banking and in some extent insurance sectors were reporting satisfactorily. Only banks reported UTRs regarding TF (effectiveness issues).

Criterion 20.1 – The reporting regime in Slovakia remains regulated by Art 17 of the AML/CFT Act which obliges the REs to report the unusual business operations (hereafter UTRs[67]) or the attempted UTR to the FIU without undue delay. The obliged person shall also immediately report to the FIU the refusal to carry out a requested unusual business operation pursuant to Art. 15. The definition of the UTR is to be found in Art. 4 of the AML/CFT Act defined as *"legal act or other act suggesting that it can be used for money laundering or terrorist financing"*. Iteration 2 of the same article lists a series of *"transactions"* that can be in particular qualified as UTR (e.g. complex, unusually high volume of funds or transactions for which the customer refuses to provide information).

The definition of UTR in the Slovak AML/CFT Act is not in line with the FATF requirements as it makes reference to *"legal act or another act"* and not to *"funds"* that might be proceeds. Hence, any suspicious funds which are not doubled by an *"act"* fall outside of the scope of the reporting obligations. Another shortcoming is the strict referral to a link to ML rather than *"proceeds of criminal activity"*. In addition, the language used to define the link of the crime is too narrow as it requires that the legal act *"can be used"* for ML purposes rather than having suspicious or reasonable grounds to suspect.

[67] The denomination of the suspicious reports in the AML/CFT Act is "unusual business operations" as described in the AT's analysis. Nevertheless, other legal and methodological acts make reference to "unusual transactions reports". As advised by the Slovak authorities and in order to avoid confusion with another largely used and well-known acronym, the AT agreed to use UTRs as the acronym for the suspicious reporting in the Slovak legislation.

Turning to the TF suspicions, apart from the shortcomings described above, another difficulty resides in the fact that the legal provisions make reference to the possibility for the operations to "be used" for TF rather than being *"related"* to TF. The deficiencies identified in the definition of TF crime further limits the application of R20.

Criterion 20.2 – There is no value threshold in the AML/CFT Act, thus, all UBO shall be reported to the FIU regardless of the amount. The attempted UTR are covered.

Weighting and Conclusion

There are moderate deficiencies in the legal obligations to report suspicious transactions, related to the definition of UTR. Moreover, deficiencies identified in the definition of TF crime further limits the application of the Recommendation. **R.20 is rated PC.**

Recommendation 21 – Tipping-off and confidentiality

In the 4th round MER Slovak Republic was rated as LC with the former R.14. The lack of precise exemption covering all civil and criminal liability when reporting suspicious transactions was the only shortcoming.

Criterion 21.1 – Pursuant to Art. 35(1) of the AML/CFT Act, neither FIs, nor their employees can be held liable for damages incurred by reporting suspicions in good faith to the FIU and they shall be presumed to have acted in good faith unless proved otherwise. There are no exemptions from civil and criminal liability for breaches of restrictions on disclosure (confidentiality requirements) imposed by contract or legislation.

Criterion 21.2 – According to Article 18(1) of the AML/CFT Act, FIs and their employees are required to keep confidential that an UTR or additional information was submitted to the FIU. This prohibition applies even after the termination of employment. Article 18(8) of the AML/CFT Act clearly envisages that this confidentiality provision does not apply to information-sharing between the FIs.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, there are no exemptions from civil and criminal liability for breaches of restrictions on disclosure imposed by contract or legislation. **R.21 is rated LC.**

Recommendation 22 – DNFBPs: Customer due diligence

In the 4th round MER, Slovak Republic was rated as PC with the previous R.12. Casinos were required to undertake CDD measures above the appropriate threshold, but not regardless of whether the transaction was conducted in a single operation or in several linked operations. Both the level of awareness of CDD obligations among DNFBPs and the outreach to the sector by the competent authorities was insufficient. The relevant legislation was revised since then and the new analysis has been undertaken.

Criterion 22.1 – The CDD requirements apply to DNFBPs in the same way that they apply to FIs, except as explained below.

(a) Casinos – Under Article 10(2)(e) of the AML/CFT Act, gambling operators are required to conduct CDD measures when undertaking transactions over EUR 2 000, whether carried out in a single operation or in several operations that appear linked.

(b) Real estate agents – According to Article 5(1)(i) of the AML/CFT Act, legal and natural persons authorized to mediate the sale, lease and purchase of real estate are obliged entities. They are

subject to general CDD requirements. They are required to apply CDD measures to whoever they have contractual relationship with (either the purchaser or vendor of the property, or both) (Art. 9(d)).

(c) Dealers in precious metals and dealers in precious stones – According to Article 5(1)(m) of the AML/CFT Act, legal and natural persons authorized to trade in precious metals and stones or products thereof are obliged entities. They are subject to general CDD requirements and thus are required to apply CDD measures when conducting cash transactions over EUR 10,000, whether carried out in a single operation or in several operations that appear linked. Also, the Law on Restrictions on Cash Payments (No. 394/2012) prohibits accepting cash payments over EUR 5,000.

(d) Lawyers, notaries and accountants – Article 5(1)(j) of the AML/CFT Act requires lawyers and notaries to apply CDD measures when they provide services related to (i) purchasing and selling of real estate or an enterprise, (ii) managing or safekeeping of funds, securities or other property, (iii) managing of bank or securities' accounts, or (iv) establishing, operating or managing of legal persons, special purpose trusts or other legal entities. Auditors, accountants and tax advisors are subject to the general CDD requirements.

(e) Trust and company service providers - According to Article 9(b) of the AML/CFT Act, the CDD requirements apply to TCSPs when providing services related to the activities listed in c. 22.1(e) except for performing the equivalent function of a trustee for other forms of legal arrangement.

Criterion 22.2 **–** DNFBPs are subject to the same record-keeping requirements as FIs (see R.11). Pursuant to Article 19 of the AML/CFT Act all obliged entities (with no exemption) are obliged to keep obtained data. Competent authorities have access to such data and information.

Criterion 22.3 **–** DNFBPs are subject to the same requirements regarding PEPs as FIs (see R.12).

Criterion 22.4 **–** DNFBPs are subject to the same requirements regarding new technologies as FIs (see R.15).

Criterion 22.5 **–** DNFBPs are subject to the same requirements regarding the reliance on third parties as FIs (see R.17).

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation. However, the deficiencies identified in relation to FIs under R.10, 11, 12, 15 and 17 are also relevant for DNFBPs. TCSPs are also not required to apply CDD measures when performing the equivalent function of a trustee for another form of legal arrangement. **R.22 is rated LC.**

Recommendation 23 – DNFBPs: Other measures

In the 4th round MER, Slovak Republic was rated as PC with the previous R.16. The shortcomings identified in relation to the previous R.13, R.15 and R.21 resulted in downgrade. The applicable legislation was revised since then and the new analysis has been undertaken.

Criterion 23.1 **–** DNBFPs, including lawyers, notaries, accountants, auditors, tax advisors, dealers in precious metals or stones, and TCSPs are required to report unusual transactions based on Article 17 of the AML/CFT Act.

Lawyers and notaries are considered obliged entities when they provide services related to transactions described in c.22.1(d) and thus, are also required to report unusual transactions. Under Articles 22 and 23 of the AML/CFT Act, lawyers, notaries, accountants, auditors and tax advisors are exempted from the reporting requirement where the professional secrecy or legal

professional privilege apply. The matters that fall under the professional secrecy or legal professional privilege broadly correspond to FATF standards;

Dealers in precious metals or stones are required to report unusual transactions under Article 14 of the AML/CFT Act;

According to Article 9(b) of the AML/CFT Act, the AML/CFT obligations, including the reporting requirements, apply to TCSPs when they providing services related to the activities listed in c. 22.1(e) except for performing the equivalent function of a trustee for other forms of legal arrangement.

Criterion 23.2 **–** DNFBPs are subject to the same requirements regarding internal controls and foreign branches and subsidiaries as FIs (see R.18).

Criterion 23.3 **–** DNFBPs are subject to the same requirements regarding higher risk countries as FIs (see R.19).

Criterion 23.4 **–** DNFBPs are subject to the same requirements regarding tipping off and confidentiality as FIs (see R.21). If lawyers, notaries, accountants, auditors and tax advisors act with a view to preventing the customer from committing an illegal act, it will not be considered as a violation of the tipping-off requirement. Also, for the sole purpose of ML/TF prevention, these DNFBPs may share UTR related information with similar entities under the joint ownership, management or compliance control that operate in other countries with equivalent AML/CFT requirements

Weighting and Conclusion

The deficiencies identified in relation to FIs under R.18, 19 and 21 are also relevant for DNFBPs. In addition, TCSPs are not required to report suspicious transactions when performing the equivalent function of a trustee for other forms of legal arrangement. **R.23 is rated PC.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

In the 4th round MER, Slovak Republic was rated as PC with the previous R.33. The BO information gathered in the process of registration of legal persons was insufficient. The FIU and some other competent authorities did not have timely access to the BO data. There were also deficiencies concerning the bearer shares. The FATF standards were amended since then and the new analysis has been undertaken.

Criterion 24.1 **–** According to Article 18(2) of the Civil Code, the following categories of legal persons can be created in Slovak Republic: trade companies and cooperatives (limited liability companies, joint stock companies, limited/unlimited partnerships, public trade companies, simple joint stock companies), foundations, non-investment funds, non-profit organizations providing generally useful services.

Information about the types, forms and basic features of legal persons, as well as their registration requirements are provided in the relevant pieces of legislation, such as the Commercial Code, the Civil Code, the Law on Foundations (No. 34/2002), the Law on Non-Profit Organizations Providing Generally Useful Services (No. 213/1997), the Law on Non-Investment Funds (No. 147/1997) and the Law on Slovak National Council (No. 207/1996).

Legal persons are registered through different registries (Commercial Register, Register of Non-Governmental Non-Profit Organizations, Register of Non-Investment Funds and Register of Foundations). The processes for obtaining and recording the basic and BO information of legal persons (except for the BO data of public entities and issuers of securities traded on a regulated

market) is provided in the Law on Commercial Register (No. 530/2003) and the Law on Register of Non-Governmental Non-Profit Organizations (No. 346/2018). These data is then transmitted to the Register of Legal Entities, Entrepreneurs and Public Authorities, which is run by the Statistical Office of Slovak Republic.

Criterion 24.2 – Slovak Republic conducted the analysis of TF risks posed by NPOs (foundations, non-profit organizations and non-investment funds) as part of the NRA. Although there is some further analysis in the NRA concerning the risks posed by different types of legal persons, this does not amount to a sufficiently comprehensive assessment of ML/TF risks associated with all types of legal persons created in the country.

Basic Information

Criterion 24.3 – All types of legal persons must be registered through the different registries noted above to be considered created. The information obtained by the Commercial Register, Register of NPOs, Register of Foundations covers all the requirements of c.24.3 and is online, thus publicly available, with one exception only (particularly, JSC shareholder data). The information contained in the mentioned Registers is available either for free in case of electronic extracts or is subject to a small fee for requesting a *"paper-form"* extract.

Criterion 24.4 – The unlimited companies, limited partnerships and limited liability companies are required to include and maintain the information on members/shareholders, as well as information on number and categories of shares in the articles of association (Sections 78, 94, 110 & 155 of the Commercial Code). Joint stock companies are either required to maintain the information on shareholders, as well as information on number and categories of shares in the company for registered shares (Section 156(6) of the Commercial Code) or submit that information to the Central Securities Depository for the book-entry bearer shares (Art. 107(8) of the Law on Securities and Investment Services (No. 566/2001)). Cooperatives are also required to keep information on their members (Section 228 of the Commercial Code). Foundations, non-profit organizations and non-investment funds are required to include and maintain the information on members in the statute or charter of the organization (Article 6&8 of the Law No. 213/1997, Article 5, 6 & 41 of the Law No. 34/2002, Article 6 of the Law No. 147/1997).

Criterion 24.5 – There are some mechanisms in place to ensure that information contained in the Registers is updated on a timely basis. The changes in the basic information must be notified in 30 days to the Commercial Register, any changes shall be entered into the Register without undue delay in case of non-profit organizations and within 15 days from the date of change in case of foundations and non-investment funds. The Commercial Register compares and harmonizes its data and entries to entries in other Registers such as the Register of natural persons or the Register of Legal Persons. Such comparison is made upon inscription of data into the Register as well as during the existence of a company. There are no other mechanisms in place to ensure that information entered into the Registers is accurate and updated on a timely basis.

Beneficial Ownership Information

Criterion 24.6 – Slovakia currently relies on combination of mechanisms to obtain beneficial ownership information. Particularly, According to Article 10a of the AML/CFT Act, all legal persons are obliged to identify their BOs, and to keep the updated BO data, and the data establishing and proving the status of the beneficial owner. These data must be kept for five years from when the person ceases to be the BO. There is no specific requirement to keep the information in the country. Besides, Slovakia has established a BO register as a centralized register for all types of legal persons. The FIU may impose a fine up to EUR 200,000 for the failure of a legal person to keep

the accurate and up-to-date BO information (Art. 33(3) of the AML/CFT Act). FIs and DNFBPs are also required to identify and take measures to verify the identity of the BO in the process of conducting CDD. However, there are no mechanisms in place to ensure that the data held by the company itself, as well as the data entered into a register pursuant to a special regulation are kept up to date.

Criterion 24.7 **–** According to the AML Act, FIs and DNFBPS are required to identify and take measures to verify the identity of the BO as described in C. 10.5. They are also required to update the documents, data and information on the customer available to them. Besides Article 10a of the AML Act requires that legal entities should identify their BOs, keep and continuously update information on them. Except for the mentioned cases, there are no other legislative provisions requiring companies and registers to check the accuracy of the beneficial ownership information. Therefore, concerns on the mechanisms used to updating information described in C.24.5 apply.

Criterion 24.8 **–** There are no specific provisions requiring companies to appoint one or more resident persons who will be accountable to competent authorities for the provision of BO information and giving further assistance, nor are there relevant provisions concerning DNFBPs. However, as noted above, legal persons are required to maintain BO information, which can then be accessed by competent authorities with some limitations (see c.24.10).

Criterion 24.9 **–** The legal persons are required to keep the BO information for five years from when the person ceases to be the BO (Art. 10a(2) of the AML/CFT Act). In addition, the obliged entities are required to retain the CDD related information (including BO information) for 5 years after the termination of the business relationship under Article 19(2)(a) of the AML/CFT Act. Excepting the Commercial Register, there is no requirement to retain the information after the company is dissolved or otherwise ceases to exist.

Other Requirements

Criterion 24.10 **–** Most of the basic information on legal persons is publicly available as noted above. According to Articles 76 and 76a of the Law on Police Force (No. 171/1993), police officers have sufficient powers to request the basic and BO information both from legal persons and relevant registries. Besides, according to Article10a(3) of the of the AML Act, when the register of legal entities entrepreneurs and public authorities does not contain the BO data or in case of doubts on the veracity or completeness of that data, a wide range of competent authorities, including LEAs can request the legal person to provide the relevant data within a specified time limit. The authorities did not explain whether the basic information on legal persons, which is not available in public registries (*e.g*. JSC shareholder data) can be accessed by LEAs in a timely fashion.

Criterion 24.11 **–** While bearer shares can only be issued in the form of book-entry securities (Art. 156(2) of the Commercial Code). The bearer shares should also be registered with the Central Securities Depository.

Criterion 24.12 **–** Nominee shareholding and directorship is not expressly regulated in Slovak Republic. However, nothing seems to prevent a person from acting as a nominee for another. Except for the requirements concerning the identification and verification of BOs while conducting CDD there are no specific regulations related to discovering the identity of the nominator by nominee shareholders or directors, licensing of nominee shareholders or directors, registering of thereof.

Criterion 24.13 – According to the Act no. 530/2003 Coll on the Commercial Register fines (up to EUR 3,310) can be imposed on a on a natural person or natural person authorized to act on behalf of a legal person who submit false or inaccurate information in the application for registration. Besides, for failure to comply with the obligations set out in Article 10a of the AML/CFT Act (keeping BO information within the company) the FIU may impose a fine of up to EUR 200,000 on the legal entity pursuant to Article 33 (3) of the AML Act.

Criterion 24.14 – The information recorded in the Commercial Register, Register of NPOs, as well as Register of Foundations and Register of Non-investment funds is available online and is either free for electronic extracts, or subject to a fee for "paper-form" extracts, and can be accessed by foreign authorities. The FIU is authorized to cooperate with foreign counterparties for AML/CFT purposes including by obtaining the shareholder data of JSCs and the relevant BO information on their behalf. LEAs can use general investigative powers to obtain the BO information on behalf of foreign LEAs

Criterion 24.15 – There are no formal processes to monitor the quality of assistance received from other countries in response to requests for basic and BO information.

Weighting and Conclusion

The Slovak Republic meets or mostly meets the majority of the criteria under this Recommendation. However, there is a number of deficiencies identified, in particular, insufficient comprehensive assessment of ML/TF risks associated with all types of legal persons created in the country; insufficient number of legislative provisions requiring companies and registers to check the accuracy of the beneficial ownership information; absence of requirement to retain the information after the company is dissolved or otherwise ceases to exist. Moreover, the legal framework does not cover sanctioning for false submissions and does not prevent a person from acting as a nominee for another. I addition, Criteria 24.15 is not met because of the absence of the formal processes to monitor the quality of assistance from abroad. **R.24 is rated LC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

In the 4th round MER, the previous R.34 was rated non-applicable. The domestic legislation did not allow for the creation of express trusts and other legal arrangements. The FATF standards were significantly revised since then and the new analysis has been undertaken.

Criterion 25.1 – Slovak Republic is not a signatory to the Hague Convention on Laws Applicable to Trusts and their Recognition. There is neither a law governing trusts or other type of legal arrangements, thus sub criteria (a) and (b) are not applicable.

There is however no prohibition on resident persons to act as trustees of express trusts formed under the foreign law. Under the AML/CFT Act a trust and company service provider are considered as obliged persons. Such services would apply de facto to foreign trusts since trusts do not exist/are not recognised under domestic law. Lawyers, accountants, auditors and tax advisors, when acting as professional trustees, are also designated as obliged entities under the AML/CFT Act (Art. 5(1)(k)). They are only required to undertake CDD measures for customers. However, the shortcomings identified in R.10 concerning the definition of BOs and their verification also impact c.25.1.

Criterion 25.2 – Trust and company service providers and other obliged entities acting as professional trustees are required by Article 10(1)(g) of the AML/CFT Act to conduct ongoing due diligence and keep the CDD documents, data and information updated.

Criterion 25.3 **–** There is a general requirement to establish the identity of the BO, which could help identify trustees in practice. However, this falls short of obliging trustees to disclose their status to FIs and DNFBPs.

Criterion 25.4 **–** Trustees are not prevented by the domestic legislation from providing the competent authorities or FIs and DNFBPs with any information relating to trusts.

Criterion 25.5 **–** LEAs are authorized to obtain information held by trustees and other parties such as FIs and DNFBPs via their general investigative powers (see R.30 & R.31). Besides, the FIU and supervisory authorities can obtain timely access to the information held by obliged entities (see R.27, R.28 & R.29). However, TCSPs are apparently not being registered as such, which could become a legal obstacle in getting access the BO data recorded in a timely manner by at least some of the competent authorities (e.g. FIU).

Criterion 25.6 **–** The ability to provide access to BO information held by domestic registries and authorities, and LEAs powers to obtain that information on behalf of foreign counterparts is discussed in c.24.14

Criterion 25.7 **–** As obliged entities under the AML/CFT Act, trust and company service providers and other obliged entities providing professional trustee services are liable for the failure to comply with CDD and record-keeping obligations. There are different sanctions, which may be applied for violations of the AML/CFT Act, including fines (up to EUR 1,000,000), publishing the legally valid decision on imposing the sanction for an administrative delinquency, and withdrawal of authorization for business activity. However, as noted above, direct obligations under R.25 for trustees are limited, and thus similarly any offences and sanctions do not clearly relate to compliance with R.25 obligations.

Criterion 25.8 **–** Trust and company service providers and other obliged entities may be subject to a fine of up to EUR 1,000,000 for failure to provide information as prescribed by Article 21 of the AML/CFT Act. Besides, other sanctions noted in c.25.7 also apply.

Weighting and Conclusion

The Slovak Republic meets the majority of the criteria, however there are a number of deficiencies in relation to trustees. In particular, the absence of legislation governing foreign trusts or other types of legal arrangements acting in Slovakia and absence of obligation for trustees to disclose their status to FIs and DNFBPs impact the overall rating of R. 25. Thus, these limitations also affect legal liability of trustees and sanctions. Moreover, the deficiencies identified in relation to BOs and their verification under R.10 are also impact this Recommendation. **R.25 is rated LC.**

Recommendation 26 – Regulation and supervision of financial institutions

In the 4th round MER, Slovak Republic was rated as LC with the previous R.23. The quality of supervision applied by the Ministry of Finance (MoF) was considered insufficient.

Criterion 26.1 **–** There are two authorities responsible for supervising and monitoring FIs' compliance with the AML/CFT requirements. Article 29 of the AML/CFT Act designates the FIU as the AML/CFT supervisory authority for all obliged entities, including FIs. Moreover, NBS is also in charge of supervising banks, insurance companies, insurance agents, payment institutions, agents of foreign payment institution, e-money institutions, securities companies, asset management companies, currency exchange operators, pawnshops, lenders, credit intermediaries other than banks an saving banks (non-banking FI) and investment pension funds (Art. 29(3) of the AML Act and Article 1 (3) and 2 (6) of the FMS Act no 747/2004)).

Market Entry

Criterion 26.2 – The NBS is responsible for prudential supervision of the entire finance sector (Art. 2(3) of the Law on National Bank (No. 566/1992); Art. 1(3) of the Law on Financial Market Supervision (No. 747/2004)). Core Principles FIs must be licensed by the NBS. Other FIs, including payment institutions and money exchange providers, are also subject to either licensing or registration. The relevant requirements are set out in the sectoral legislation (Law on Banks (No. 483/2011), Law on Payment Services (No. 492/2009), Law on Foreign Exchange Services (No. 202/1995), Law on Insurance (No. 39/2015), Law on Securities (No. 566/2001), Law on Supplementary Pension Scheme (No. 650/2004)) and Law 129/2010 on consumer credits and loans for consumers (leasing companies).

There is no explicit prohibition on the establishment or continued operation of shell banks. However, the Law on Banks (Art. 7(2)(k)) requires that a bank's registered office, headquarters, and place of business must be on the territory of Slovak Republic. Although, physical presence of the meaningful mind and management is not specifically required.

Criterion 26.3 – The NBS applies certain fit & proper criteria to shareholders and managers of FIs based on sectorial legislation (Art. 7(10) (14-15) (16-7) of the Law on Banks; Art. 2(27)(30-31) of the Law on Payment Services; Art. 6(3)(5) of the Law on Foreign Exchange Services; Art. 24 and Art. 181 of the Law on Insurance; Art. 8(b), Art. 56(12), Art. 58(2) and Art. 70(8) of the Law on Securities, Art. 23 (4), (12) of the Law 650/2004 on the supplementary pension scheme, Art. 48 (4), (12), Law 43/2004 on the old age pension scheme, Art. 28 (4), (5), (7), (11) of the Law 203/2011 on the collective investment, Art. 4 (4), (12) of the Law 439/2002 on Stock exchange, Art. 20a (3), (12), Art. 20b (5), Art. 24 (7) of the Law 129/2010 on consumer credits and loans for consumers).

The NBS has also issued various Decrees (NBS Decree no. 12/2008 Establishing the method of proving the fulfilment of conditions for granting a licence to provide ***investment services*** , Decree no 16/22 November 2011on the elements of a ***banking licence*** application made by a ***bank or branch of a foreign bank*** and on how to prove compliance with the conditions for such licence and amended by Decree no. 3/ 6 February 2018, Decree no. 6 December 2012 on how to demonstrate compliance with conditions for an authorisation to act as a ***management company***, Decree no 139/14 may 2013 laying down detailed provisions on the elements of an application for a ***foreign exchange licence*** and on requirements for trade in foreign exchange assets , Decree 8/4 august 2015 establishing a method for proving compliance with the conditions for granting an authorisation to conduct ***insurance business*** and authorisation to conduct reinsurance business for entities which will not be subject to a special regime , Decree no 35/15 December 2015 concerning the method by which ***insurance undertakings*** subject to a special regime are to demonstrate compliance with conditions for the granting of an authorisation to conduct insurance business, Decree no 162/29 may 2012 on how to demonstrate compliance with conditions for an authorization to establish and operate ***a pension fund management company***, Decree no 1/25 September 2018 on the register of financial agents, financial advisers, financial intermediaries from other Member States operating in the insurance or reinsurance sector, and financial intermediaries from other Member States engaged in the provision of housing loans) on applications, approval of persons and the manner to substantiate ***fitness & properness of persons.***

When licensing banks, NBS checks trustworthiness / criminal record ("*a natural person who has not been convicted for a criminal offence against the right of property, for a criminal offence committed in relation to a managerial function performance or for a wilful criminal offence; these facts are proved by means of a criminal record transcript; where this concerns a foreign national,*

these facts are proved and documented by an equivalent document not older than three months issued by a competent authority in the country of which this person is a national or by a competent authority in the country in which this person's permanently or habitually resides") of members of the statutory body, administrative board and supervisory board, as well as other senior executives. Similar measures are applied in case there are new appointment for the abovementioned positions. This does not however cover the *associates of criminals.*

The NBS does not subject persons holding a significant or controlling interest or management function in an FI to ongoing monitoring and is reliant on its licensed community to self-report any changes.

The NBS also checks whether holders of the significant interest (20%) in a bank are suitable persons i.e. are able to properly and safely conduct business activities in the interest of stability of the banking sector. This is being done both during the licensing and when granting the prior consent to the acquisition of the significant holding in a bank. The authorities did not explain what specific measures are undertaken to prevent criminals or their associates from holding or being the BO of the significant interest in a bank as part of the suitability checks. Nevertheless, criminal records of the applicants are verified by the NBS in practice.

In relation to insurance undertakings, the NBS examines the criminal record (conviction of criminal offences related to property or management) of persons holding key management functions both at the licensing stage and later, when changes occur (based on the notification of the entity or during the onsite supervision). The insurance sector takes into consideration also ongoing criminal prosecutions when assessing the fitness and properness of a natural person. This is however not sufficient to guard against the associates of criminals. The NBS also checks the eligibility of owners of the significant holding (20%, 30% or 50%) in an insurance undertaking. The eligibility checks are aimed at obtaining evidence that an undertaking will be run in a reliable and prudent way. No information was provided about specific measures to prevent criminals or their associates from holding or being the BO of the significant interest in an insurance undertaking.

Investment firms must assess a set of elements (including a criminal record proving that the person was not convicted of a crime committed in connection with the performance of a managerial duties or a deliberate crime) in order to determine the good reputation of a natural person for a period of 10 years (article 8 b) of Act on securities

Payment institutions (MVTS), electronic money institutions, bureaux-de-change are obliged to inform the NBS about any criminal record concerning its management (management includes members of statutory body, director or any other person managing the entity) as well as information on any changes regarding members of management including information that allows the NBS to verify if such newly nominated member of management has any criminal record by checking the Criminal Register. For a foreign national an extract from the criminal record (or any equivalent document) of his home country has to be provided to the NBS (Article 2 (31) and (54_ of the Payment service act).

Risk-based approach to supervision and monitoring

Criterion 26.4 – a) The Basel principles for effective banking supervision have been implemented through the EU Regulation 2013/575 on prudential requirements for credit institutions and investment firms, although Slovak Republic was not subject to any rated assessments therein. The authorities stated that the NBS is a member of IAIS and IOSCO and thus, applies about the implementation of IAIS principles or IOSCO principles and responsibilities.

(b) In relation to FIs, other than core principles institutions, the authorities did not explain the systems for monitoring and ensuring compliance with national AML/CFT requirements and whether they are risk-based.

Criterion 26.5 **–** The NBS has in place a procedure for banks that governs the on and off-site supervision of credit institutions. According to the procedure the following issues are considered for making a decision on the scope and criteria of the AML/CFT onsite inspections of the banks:

The concept and basic principle of protection against money laundering and financing terrorism;

The AML/CFT responsible employee;

The banks programme aimed to protect against money laundering and terrorism financing;

Awareness and education of employee, information system;

Client identification, CDD, client risk profile, correspondent relationship, reliance on third parties;

Detection, blocking and reporting suspicious transactions;

Counter measures against terrorism financing;

Record keeping.

The NBS has in place a similar procedure for payment institutions, electronic money institutions, insurance and capital markets. The risk-based supervision exercised by the NBS takes into consideration when classifying the FI, factors and vulnerabilities laid down in the Slovak Republic NRA. According to the article 26a of the AML Act, the NRA is to be updated with respect to the development of risks of money laundering but there is no actually risk classification or risk mapping of the FIs supervised.

The NBS has legal powers to supervise (on site and off site supervision) financial institutions from an AML perspective so it should take in mind the AML risk factors (client, product and distribution channel, jurisdiction) and organize it's supervision, staff, monitoring having in mind an AML risk framework, a classification of the financial entities according to the risks identified and assessed (risk map), a risk matrix, implement a monitoring process for each category of entities and AML sanctions.

The risk classification is informed by the NRA and the information obtained via off-site supervision (questionnaires and internal control reports of the entities) and on-site inspections. The NBS also takes into account the specific characteristics of individual entities, such as their market share, ownership and control structure, products and distribution channels, geography of business activities, high-risk customers and the quality of compliance function. The frequency of supervision is then determined based on the assigned risk level. In particular, higher-risk insurance undertakings are subject to annual off-site supervision and on-site inspections. The risk classifications/profile however do not affect the intensity or scope of supervision applied to individual insurance undertakings.

The Slovak FIU is always informed by the NBS before conducting onsite inspection according to the AML Act. Furthermore, the supervisory team (NBS staff) during the onsite inspection focuses on the AML/CFT internal procedures for the application of CDD measures (customer risk profile taking into consideration the AML/CFT risk factors), reporting of the suspicious activities, record keeping and ongoing monitoring.

The FIU does not have any ML/TF risk/based procedures that drive frequency and intensity of on-site. As for the off-site AML/CFT supervision, the FIU does not conduct off-site supervision.

Criterion 26.6 **–** As noted above, the NBS is using the results of off-site supervision and on-site inspections, and findings of the NRA to determine ML/TF risk profiles of financial entities. There was no information provided about the revision of individual ML/FT risk profiles or those of financial groups when major events or developments take place in the management and operations therein. The FIU does not have any procedure reviewing the assessment of the ML/TF risk profile of a financial institution.

Weighting and Conclusion

There are no actual documented risk classification/risk profile or risk matrix and the frequency and intensity of onsite or of site AML/CFT supervision of financial institutions/group are based on an investigation plan (annual plan) not on the ML/TF risks. Moreover, the NBS and the FIU do not have any formally approved criteria for determining the frequency and intensity of on-site and off-site AML/CFT supervision of financial institution of groups. There are also shortcomings related to the requirements for the NBS to perform checks with respect to the associates of criminals. **R.26 is rated PC.**

Recommendation 27 – Powers of supervisors

In the 4th round MER, Slovak Republic was rated as LC with the previous R.29. There was not enough focus placed on the information requirements concerning wire transfers during on-site visits by the NBS.

Criterion 27.1 **–** The FIU is designated as the supervisory authority and is responsible for ensuring compliance of FIs with the AML/CFT requirements (Art. 29 of the AML/CFT Act). The NBS also conducts the supervision of FIs on the basis of the Law on Financial Market Supervision. Its supervisory powers are set forth in the sectorial legislation (Art. 6 of the Law on Banks; Art. 60 of the Law on Payment Services; Art. 24 of the Law on Foreign Exchange Services; Art. 79 of the Law on Insurance; Art. 135 of the Law on Securities).

According to Article 4 of the Law on Implementation of International Sanctions (No. 289/2015), the FIU and NBS have powers to supervise and ensure compliance of FIs with requirements on the implementation of UNSCR sanctions.

Criterion 27.2 & 27.3 **–** The FIU is authorized to conduct inspections pursuant to the AML/CFT Act (Art. 29). This includes the ability of the FIU inspectors to visit premises, compel production of documents and obtain access to electronic systems of inspected entities. The latter are further required to create necessary conditions for the FIU inspectors and to refrain from actions that may frustrate their efforts (Art. 30). The NBS also has the authority to conduct on-site inspections of FIs by entering their premises, testing AML/CFT systems and obtaining relevant documents (Art. 1(3)(a) of the Law on Financial Market Supervision (No. 566/1992)).

Criterion 27.4 **–** Article 33 of the AML/CFT Act gives the sanctioning power to the FIU. Available sanctions include imposing fines up to EUR 5,000,000 (Art. 32), requiring the publication of the decision to apply a sanction and relevant circumstances (Art. 33), and requesting the relevant authority to withdraw the authorisation (license) for serious or consecutive violations (Art. 34). In determining the amount of a fine, the FIU must take into account the seriousness, duration and consequences of the violation(s), as well as the level of cooperation provided by and size of the supervised entity. The NBS has also the power to impose sanctions for breaches of AML/CFT

requirements, and is required to inform the FIU of any AML/CFT violation uncovered during the supervision to avoid double sanctioning.

The FIU is in turn required to notify the NBS about the follow-up measures/sanctions applied (Art. 29(4) of the AML/CFT Act). The authorities did not explain the legal processes for withdrawing, restricting or suspending the FIs' license for AML/CFT violations.

The authorities stated that the NBS shall take into account the severity, duration and consequences of uncovered violations when considering the FIU's request to withdraw the authorization (license) of banks and securities market intermediaries (Art. 50(1) of the Law on Banks).The authorities did not explain the legal processes for withdrawing, restricting or suspending the license of other FIs' for AML/CFT violations.

Financial sectors:

In the event that the Financial Intelligence Unit submits to NBS an incentive to withdraw the authorisation of an entity supervised by NBS (insurance companies, insurance agents, payment institutions, agents of foreign payment institution, e-money institutions, securities companies, asset management companies, currency exchange operators, pawnshops, lenders, credit intermediaries other than banks and saving banks (non-banking FIs) and investment pension funds), NBS shall examine such an incentive and, within 30 days of receipt of the complaint, notify the FIU about the method of solving the complaint.

Withdraw authorisation to carry out the activities of entities supervised by NBS shall be authorised only by NBS in accordance and subject to compliance with the conditions laid down in the special rules governing the exercise of supervision of the financial market (e.g. Securities Act-§ 156, Insurance Act - § 158, Old-age Pension Law Act - § 120, where is stipulate when NBS has to withdraw the authorisation and when it can withdraw the authorisation).

In the case of investment firms, NBS takes into account when determinate the type of sanction the seriousness, duration of the deficiency, the person's responsibility, the financial situation of the person responsible, the level of cooperation, previous infringements and the measures taken after breach of law (§ 144 of Securities Act). The incentive to withdraw the authorisation submitted by the Financial Intelligence Unit is not sufficient for the withdrawal of the authorisation and NBS must have proven shortcomings by it´s own activities (supervision).

In the case of insurance companies, the NBS may, depending on the severity, extent, duration, consequences and nature of the deficiencies identified (§ 139 of Insurance Act), withdraw the insurance undertaking or branch of a foreign insurance undertaking to carry on insurance activity for certain insurance industries foreign insurance company, which simultaneously carries out life insurance and non-life insurance, authorization to carry out insurance activities for life insurance or non-life insurance. The NBS may also revoke an authorization to an insurance company even if the sanctions imposed pursuant to this Act or a special regulation have not remedied the identified deficiencies (i.e., theoretically also on the basis of an FSJ initiative of repeated violation of AML / CFT regulations).
In the case of pension companies, the NBS may revoke the license for pension companies to establish and operate them, based on the nature, severity, manner, degree of fault, duration and consequences of the breach (§ 115 of Old – age Pension Law Act). As regards the FSJ's initiative for withdrawal of authorization, the same is true of investment firms.

OFI:

Pursuant to Section 39 of the Act No 186/2009 of 24 April 2009 on financial intermediation and financial advisory services if NBS finds any deficiencies in the activities of a financial agent or of a financial adviser or of a proposer, consisting in non-compliance with the conditions or obligations arising from decisions issued by NBS or in non-compliance with, or circumvention of, the provisions of this Act, other legislation within the scope specified therein, and of the legislation of general application issued for their implementation, which apply to the provision of financial intermediation and financial advisory services by these persons, NBS may take the following steps: impose measures on the financial agent, financial adviser or proposer in question, designed to eliminate or remedy the deficiencies revealed, including a time limit for their implementation, and require them to inform NBS of the fulfilment of this requirement within the prescribed time limit; charge the financial agent, financial adviser or proposer a fine of up to EUR 5,000,000 or up to 5% of their total annual turnover according to the last available financial statement or up to twice the amount of the profits gained or losses avoided because of the infringement, where those can be determined, in the case of a legal person, or a fine of up to EUR 700,000 or up to twice the amount of profits gained or losses avoided because of the infringement, where those can be determined, in the case of a natural person; require the independent financial agent or financial adviser concerned to restrict or suspend their activities in some sectors; revoke the independent financial agent's or financial adviser's authorisation under Section 18 or restrict their authorisation under Section 18 in relation to some sectors; remove the tied financial agent, subordinate financial agent or tied investment agent from the relevant register; release a public statement indicating the natural or legal person responsible for the infringement, and the nature of that infringement; impose a temporary ban against the natural person who is held responsible for the infringement, to perform managerial functions while working for the financial agent or financial adviser in question.

Pursuant to Section 19 (1) (g) of the Act No 186/2009 of 24 April 2009 on financial intermediation and financial advisory services setting out the expiry of an authorisation to act as an independent financial agent or as financial adviser, an authorisation to act as an independent financial agent or an authorisation to act as a financial adviser shall expire on the effective date of the decision on the withdrawal of such authorisations.

Weighting and Conclusion

The Slovak Republic meets most of the criteria under this Recommendation, but there was no information provided about the legal framework for withdrawing, restricting or suspending all FIs' license for AML/CFT violations. **R.27 is rated LC.**

Recommendation 28 – Regulation and supervision of DNFBPs

In the 4th round MER, Slovak Republic was rated as PC with the previous R.24. There was no clear strategy concerning the DNFBP supervision and the outreach to the sector was also insufficient. The FATF standards were revised since then and the new analysis has been undertaken on 29 January 2019, the Slovak parliament adopted a new Gambling Act (Law 30/2019 effective from 1st of March 2019. The new Gambling Act opens Slovakia's online gambling market and allows private companies, as well as online operators based in other EU markets, to apply for licences to run online casino games.

Criterion 28.1 – a) and b) Casinos and online casinos are subject to licensing by the Gambling Supervisory Authority Pursuant to Art. 48 (4) of the new law, for obtaining an individual license the applicant must, inter alia, possess integrity ((a) the person who was not sentenced for an economic crime, crime against order public matters or a crime against property; (b)other wilful criminal act.). Integrity must be proved also by legal persons registered in SR or in other EU

member (using an extract from the Criminal Record or an equivalent document). The measures of the new gambling law also do not cover the associates of criminals.

c) The AML/CFT Act designates the FIU as the AML/CFT supervisor for casinos (Art. 29) . The FIU has the power to conduct onsite visits and obtain access to any document or electronic systems of the supervised entity (Art. 30). According to Article 11 of the Law on Gambling Games, the casinos are also supervised by a number of other supervisory bodies such as the Financial Directorate, and the tax and customs services (until 2016 the MoF performed AML/CFT inspections and since 2016 the Tax authorities were in charge of AML/CFT inspections). Pursuant to the new Gambling law all the off-site and on-site supervision prerogatives were transferred to the new Gambling Regulatory Authority.

Criterion 28.2-28.3 **–** The FIU is the designated competent authority responsible for monitoring the compliance of all categories of DNFBPs with AML/CFT obligations. As described above, the FIU has adequate powers to conduct onsite inspections and obtain required data (according to the new gambling law the on-site inspections can be performed also by the new gambling authority).

Criterion 28.4 **–** a) The FIU has adequate powers to monitor compliance of DNFBPs with AML/CFT requirements by conducting onsite inspections and obtaining any required data or documents.

b) Professional licenses granted by SRBs to auditors, tax advisors, accountants, notaries, lawyers, bailiffs, real estate agents and dealers of precious metals and stones require the absence of criminal record. This however would not prevent the criminals' associates from entering the professions.

c) The AML/CFT Act provides the FIU with the sanctioning power. Available sanctions include imposing fines up to EUR1,000,000 (Art. 33), requiring the publication of the legal valid decision/applied sanction (Art.33a) and requesting the relevant authority to withdraw authorization/license for serious or consecutive violations (Art. 34). The range of these sanctions appears adequate; however, they concern only the entities and do not apply to persons performing managerial functions therein. In addition, the SRBs can withdraw the professional licenses granted to auditors, tax advisors, accountants, notaries, lawyers and real estate agents for violating the licensing conditions related to the absence of criminal record. (the new gambling law provides sanctioning prerogatives to the new gambling authority).

Criterion 28.5 **–** The relevant regulation and inspection guidance of the FIU do not provide for determining the frequency and intensity of supervision on a risk-sensitive basis. The FIU inspectors are required to understand certain characteristics (size, distribution channels, ownership structure, etc.) and risk factors related to DNFBPs before conducting an inspection (FIU Order No. 297/2008). This however does not equal to the risk-based assessment of the adequacy of internal controls, policies and procedures of DNFBPs.

Weighting and Conclusion

Slovakia meets criteria 28.2 and 28.3 and partly meets criteria 28.1, 28.4 and 28.5. Since there are a number of deficiencies: No measures in place to prevent associates of criminals from holding management functions in DNFBPs. There are no checks applied in relation to holders or BOs of significant or controlling interest in DNFBPs; The sanctions for violations of AML/CFT requirements do not apply to persons performing management functions in DNFBPs; The frequency and intensity of supervision over DNFBPs is not determined on a risk-sensitive basis. **R.28 is rated PC.**

Recommendation 29 - Financial intelligence units

In 2011 MER Slovakia was rated PC with the former FATF Recommendation 26. The main deficiencies were: concerns of the weak position of the FIU in the police structure and the system as a whole, lack of legal safeguards for its operational independence, annual reports did not contain information on trends and typologies and an insufficient focus on ML and TF, but rather on all criminal offences equally. It was not possible to assess effectiveness since statistics were related to all criminal offences.

Criterion 29.1 – Slovak FIU is established through Art. 29a (5) of the Act 171/1993 Coll. on Police Force (hereafter the Act on Police) as a special division of the Financial Police which *"performs tasks related to prevention and detection of legalisation of incomes from criminal activities and terrorism financing pursuant to special regulation"*. The Act on Police does not clearly identify the *"regulation"* setting up the FIU, but the authorities advised that in this case the *"special regulation"* shall be considered the AML/CFT Act. Nevertheless, the AT notes that there is no legal provision clearly determining that the *"special division of the Financial Police"* as defined by the Act on Police is actually the FIU referred to in Art. 26 of the AML/CFT Act. The only law making the link between the Art. 29a (5) of the Act on Police and the AML/CFT Act is the Law 199/2004 on Customs Code which quotes: "The customs office shall send the completed forms under paragraph 2 to the *financial intelligence service* of the Police Force".

Art. 26 (2) (a) AML/CFT Act, provides that the FIU fulfils the tasks of a central national unit in the area of preventing and detecting money laundering and terrorist financing. Amongst the powers and responsibilities of the FIU are: receive, analyse, evaluate and process unusual business operations and other information related to money laundering and terrorist financing, and assign the matter to law enforcement authorities if the facts suggest that a crime has been committed. There are no competences assigned to the FIU related to associate predicate offences. To the later, the Slovak authorities argued that the competence of the FIU in the environment and conditions of the Slovak Republic cannot be defined only from the point of view of legalization of proceeds from crime, as FIU employees/police officers are also members of Police Force, who check and detect various criminal activities, especially of economic nature (not only legalization of proceeds from crime). In the light of the explanations provided by the authorities, corroborated with the findings on the dissemination process (see EC 29.5), the AT concludes that the requirement related to the predicate offences is met.

Criterion 29.2 – As described above the AML/CFT Act (Art. 26 (2) (a)) provides that the FIU shall receive, analyse, evaluate and processes reports of unusual business operations and other information related to money laundering and terrorist financing, filed by the RE. Apart from the UTRs, the only threshold reports received by the FIU are customs declarations for cash above EUR10,000. According to Art. 4 (4) of Law 199/2004 on Customs Code, the customs office shall send the completed cash declarations forms to the financial intelligence service of the Police Force by the fifth day of the calendar month following the month in which these facts occurred.

Criterion 29.3 – a) Based on the FIU written request and for the purposes of fulfilment of its tasks pursuant to the AML/CFT Act, the obliged person shall provide the FIU with the data on business relationships or transactions, submit documents, and provide information on the persons that took part in the transaction in any way (Art. 21 (1)). The FIU shall provide the time-limit for the completion of the request (which the authorities stated is usually of 7-14 days). However, this precise period does not follow from any provision of the AML/CFT Act. The AT could not identify a provision allowing the FIU to "use" the additional information received from the REs. In addition,

since strategic analyse is not specifically recognised as an FIU task, there is no ability to collect all the necessary data for this purpose.

b) According to Art. 76 of the Act on Police, the PF units (which would include the FIU) are entitled to request documents and information from state authorities, municipalities, legal and natural persons when performing their tasks. In practice, the FIU has access to a series of DB such as: Register of investigated cases (DVS), the Commercial Register, the Slovak population register,; record of drivers, vehicles; cadastral portal; Register of wanted persons, BO register, Register of public sector partners, Trade register, Register of foundations, non-investment funds and NPO register, Finstat and Register of Financial Statements (see also analysis under IO6)

Criterion 29.4 – a) The FIU is empowered to conduct operational analysis as required by 29.4(a). The Order of the Director of the FIU on "The Method of implementation of some provisions of the AML/CFT Act" from 2018 (hereafter The FIU Methodological Order) stipulates the UTR prioritisation mechanism (in three categories depending on the risk) and the steps to be taken in conducting analysis. The analytical process requires: further information on the UTRs from REs, search for and identify all transactions, financial flows, natural and legal persons that are relevant for further assessment, ensure other relevant information and evidence through available registers and databases and also open sources, ask foreign FIUs for cooperation, and prepare the analytical report. At the operational level, the FIU uses a number of analytical tools. The analysis is performed by the UTR Department.

b) The FIU's Analytical Unit in collaboration with other departments develops strategic analysis on new phenomena of crime. The FIU Methodological Order provides that the UTR Unit shall provide the Analytical Unit with the information needed to develop strategic analyses, the results of which are published in the FIU's Annual Report. No other details on what the *"strategic analysis"* shall include, or on the activities of the Analytical Unit are provided. The AT notes that, in spite indirect referrals to *"strategic analysis",* there is no clear legal obligation for the FIU to carry out strategic analyses to identify money laundering and terrorist financing related trends and patterns.

Criterion 29.5 – The FIU has the ability to disseminate spontaneously and upon request specific information to competent authorities. The dissemination provisions are stipulated by four different items in the AML/CFT Act which are not fully clear and overlapping, creating effectiveness issues in practice (see IO6). The authorities advised that the following distinction between the three items apply:

> According to Art. 26 (2) (b) of the AML/CFT Act, the FIU shall submit information to law enforcement authorities if facts suggest that a crime has been committed. According to the authorities, these concern the cases where there are findings or suspicions regarding the commission of a specific criminal offence with a presumed damage.
>
> According to Article 26 (2) (l) of the AML Act, FIU submits information to the Police Force for further utilization pursuant to a special regulation. These concern the UTRs and the cases with a lower level of substantiation on the underlying criminality and are usually used by LEA for information or for "operative" purposes and pertain mostly to potential tax frauds.
>
> According to Art. 26 (2) (j) of the AML/CFT Act, the FIU provides information to the tax administrator and government authorities in the area of taxes, fees and customs if the information is relevant and such provision does not endanger the fulfilment of the tasks of the FIU,

According to Article 26 (3) of the AML Act, FIU provides all the information and documentation it has received under that law to the State authorities which carry out tasks in the field of protection of the constitutional system, internal order and security of the state for fulfilling their statutory tasks in the fight against terrorism and organized crime.

Art. 4 (3) of the FIU Methodological Order, provides guidance on dissemination. The Slovak authorities stated that all information obtained from UTR reports is collected in the FIU's system DMS. The e-mail communication in protected mode, encrypted form using suitable means with the help of mutually exchanged encryption keys, which allow only the respective recipient to open the e-mail communication, is provided for the receipt and also distribution of information in electronic form. Nevertheless, there are no formal legal provisions regulating the obligation to use dedicated, secure and protected channels for disseminations.

Criterion 29.6 – a) According to Article 18 (4) of AML/CFT Act the obligation of secrecy shall apply to everyone who becomes familiarised with the information obtained based on this Act, while fulfilling the tasks of the FIU, or in connection with them. Art. 18 (11) of the AML/CFT Act provides that the authorities who receive the FIU disseminations shall be obliged to keep secret information and documentation provided under Art. 26 (3) of the AML/CFT Act.

The procedure for handling information - UTR reports (their receipt, registration, procedure and method of handling, analysing, feedback, duty not to disclose) are regulated by the FIU Methodological Order. The information gathered by means of encrypted e-mail communication is inserted into the DMS (system without Internet access), by a designated employee of the FIU. Same goes for UTRs received in a written form. Only registered users - FIU workers with their own login data - can access the DMS. Depending on the respective FIU department, privileges are granted to allow access to the system according to the protocol. The senior staff is allowed to view all files of subordinate employees.

The communication with foreign FIUs is via encrypted communication channels Egmont Secure Web (ESW) and FIU-net. Terminals (computers) for both systems are in a separate room that only the staff of the International Cooperation Department can access. Acquired information from ESW and FIU-net encrypted mail is inserted in the closed DMS system by the designated staff of the International Cooperation Department.

At NAKA level, the archives shall be constantly locked and if the premises are equipped with an electric security system, the coding shall be activated. Entry of authorised persons to such premises is the responsibility of the authorised person to whose care have the premises been assigned. Nevertheless, there is no specific legal provision on how the FIU files are handled and stored, and whether this shall be physically distinct from other police units.

Another matter for concern is the protection of disseminated information, as according to the AML/CFT Act, the dissemination of FIU products is quite wide ranging from *"authorities responsible for constitutional establishment protection, internal order and state security"* to the Police Force performing tasks under a special regulation. The FIU Methodological Order under point 7 mentions that if the FIU employee finds that the UTR report information is relevant for any part of the Police Force that performs the tasks under a special law[2], he/she shall send it to the competent component. Special law in this case is Art. 2 of the Act on Police Force which lists all police force tasks, including safeguarding public order, protecting personal security of important persons, and disclose minor offences and identify their perpetrators.

b) The FIU police officers are obliged to maintain confidentiality about the facts they learnt in the course of or in connection with the tasks of the Police Force (Art. 80 (1-3)) Act on Police Force. The

confidentiality obligation does not apply to the notification of crime or other anti-social activity. The Minister or the President of the Police Force may discharge a person from the confidentiality obligation. There are no security clearance requirements for FIU staff but this derives indirectly from an internal order issued by the FIU Head in August 2019 corroborated with the provisions of the Act No. 215/2014 Coll. on the protection of classified/confidential information. Pursuant to the Order of FIU 4/2019 on the list of functions for which authorized persons may access classified information, there are 36 management and execution level positions that can have access to "Confidential" information. The Act on protection of classified/confidential information foresees the obligation of each statutory body handling confidential information to request the National Security Bureau to carry out Levels II through IV security clearance of those nominated as persons authorised to be provided with access to classified information at the Confidential.

c) There is limited and protected access to FIU facilities and information, including IT systems. Contactless cards are assigned to specific personal number of the FIU employees. Entrance areas are monitored and the FIU servers are cut-off from external networks.

Criterion 29.7 – a) The 4th round MER describes the concerns related to the operational independence of the Slovak FIU. Since August 2019 the FIU of the Slovak Republic was subject to structural changes inside the Police organizational scheme and is now under the direct supervision of the President of the Police force. The FIU has increased its level of independence by having its own budget item in the overall Police Force budget and the FIU Director acquired the power to employ staff on its' own decision. The Director of the FIU is appointed by decision of the Director of the President of the Police force. The decision to analyse, request, and/or forward or disseminate specific information belongs to the FIU management. However, the unclear provisions on disseminations open the door for potential abuse in terms of full control and autonomous decision to disseminate.

b) The FIU is authorized to cooperate independently under Art. 26 (2 (b, j, k, l and m)) and (3) of the AML/CFT Act – with internal counter-parts. Nevertheless, the text of the articles above, make reference to information provided by the Slovak FIU and not information exchange in general (the ability to request and receive information is absent). The authorities argued that the FIU asks for information from competent entities outside the Police Corps pursuant to art 76 para. 1 of the Police Corps Act. Nevertheless, it is still unusual that the two ways of communicating be regulated by different pieces of legislation. The ability of the FIU to conduct international cooperation (including with foreign FIUs) on the basis of international treaties binding Slovakia and on non-contractual reciprocity principle is stipulated in Art. 28 of the AML/CFT Act. The FIU, as a department of PF, is entitled to cooperate with domestic actors in the virtue of Art. 3 of the Act on Police Forces. The FIU is also able to agree on cooperation with national competent authorities and foreign partners on a contractual basis. Nevertheless, while there is quite wide legal base for information exchange, the Head of the FIU is not able to conclude MOUs independently.

c) The special position of FIU within the Police Force is derived from the provision of Article 29a (5) of the Act on the Police Force in conjunction with Article 26 (1) of the AML Act and ensures distinct core-functions from those of another authority. The FIU does not fulfill any other tasks that are entrusted to other units of the Police Force. Nevertheless, the AT is of the opinion that the FIU's position and core-functions definitions are quite volatile as the Act on the Police Force is linked to other acts, while the FIU underwent frequent reorganizations in several units/departments of the Police Force: Financial Intelligence Department of the Financial Police Bureau of Police Force Presidium (from 11.1996-12.2003), Intelligence Unit of Financial Police of the Bureau for Combating Organized Crime of Police Force Presidium (from 01.2004-11.2012), Financial

Intelligence Unit of National Criminal Agency of Police Force Presidium (from 12.2012-07.2019), Financial Intelligence Unit of Police Force Presidium (since 01.08.2019). As a result, the various pieces of regulations are not harmonized and reference is made to the FIU in a very inconsistent manner throughout the legislation.

d) Until August 2019 the FIU did not have its own budget, but the authorities maintain that the FIU was able to obtain the resources needed to fulfil its tasks through planning documents. After the latest reorganisation (August 2019), the FIU has its own budget, but this will be functional in the next budgetary exercise, hence for effectiveness purposes this would not apply for the evaluated interval. On the basis of this change, the Economy Section of the Ministry of the Interior of the Slovak Republic designated the FIU as a cost center for the administration of state property and at the same time in the integrated accounting information.

Criterion 29.8 – The Slovak FIU has been a member of the Egmont Group since June 1997.

Weighting and Conclusion

Slovakia meets most of the requirements under R.29 and only moderate shortcomings remain. There are concerns about the operational independence of the SR FIU due to the inconsistent manner in which the FIU is defined throughout various pieces of legislation and other regulations and repeated changes within the Police structure. The Head of the FIU is not able to conclude MOUs independently. The strategic analysis is not specifically defined and there are deficiencies in the protection of disseminated information and in relation to the formal requirements on the physical archive of the FIU files. **R.29 is rated PC**.

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

Slovakia was not assessed for former Recommendation 27 as in the 3rd round it was rated LC. The *reserve pertained to the effectiveness of money laundering and terrorist financing investigations.*

Criterion 30.1 – There are no designated LEAs in Slovakia with specific responsibility to investigate ML offences. Within the Slovak Police Force, investigators of each NAKA Unit (such as ARO NAKA, Anti-Corruption NAKA) as well as the National Unit to Combat Irregular Migration or the units of the Criminal Police Service are primarily responsible for investigating the predicate offences falling under the competence of the respective police body, but they are also authorized to investigate any ML offence committed in relation to these predicate offences.

Criterion 30.2 – As part of the investigation of the predictive crime, the investigator may also investigate the related ML case. Thus, it is not excluded that one investigator conducts an investigation for both a predictive offense and an ML offense. In case the ML case appears to be outside of the competence of a certain LEA, the case can be referred to the higher-rank unit within the regional Criminal Police Department or NAKA, while the investigation of the predictive crime could still be investigated by the original investigator. In these cases, the separate criminal proceeding will be conducted as stipulated by the Article 21 of the CCP.

As with regard the competence for the financial investigation applies mutatis mutandis. The investigator is solely responsible for the investigating file, as well he or she is exclusively authorized to conduct the evidence in the ML investigation file incl. financial investigation (applies mainly for the District Criminal Police).

Criterion 30.3 – There is no specialized Police unit or other authority to carry out identification, search and seizure of suspected criminal proceeds or property subject to confiscation. These procedural acts are carried out by all LEAs investigating proceeds-generating cases, in line with

Art. 119 (1)(f) of the CCP which requires the authorities to prove if there are proceeds from the respective criminal activity.

This is assisted by the ARO NAKA which is also the designated ARO of Slovakia (the ARO was part of the FIU until 2017). This Department elaborates property profiles of natural or legal persons for other NAKA units with the aim of detecting and identifying assets or proceeds of crime. Provision of such assistance to LEAs other than NAKA, however, depends on the discretion of the NAKA Director, requiring a case by case approval pursuant to Art. 3(2) of the Guideline of the NAKA Director No. 57/2017 which restricts its availability for all LEAs investigating proceeds-generating crimes.

Criterion 30.4 – There are no such authorities in Slovakia.

Criterion 30.5 – The Slovakian anti-corruption LEA is the Anti-Corruption NAKA, which is designated to investigate associated ML and TF offences, by virtue of selective competence as mentioned above under c.30.1 and which has sufficient powers to identify and to initiate the seizure of assets.

Weighting and Conclusion

There are no designated LEAs in Slovakia with specific responsibility to investigate ML offences. The LEA investigators are authorised to pursue ML offences during a parallel financial investigation. There is no specialized Police unit or other authority to carry out identification, search and seizure of suspected criminal proceeds or property subject to confiscation which acts are carried out by all LEAs investigating proceeds-generating cases. The Anti-Corruption NAKA has sufficient powers to identify and to initiate the seizure of assets. **R.30 is rated PC.**

Recommendation 31 - Powers of law enforcement and investigative authorities

The last time Slovakia was assessed against the then Recommendation 28 was in the 3rd round of MONEYVAL evaluations (2006) when it was found to Compliant. This recommendation has been further expanded by introducing requirements for countries to have mechanism in place to identify whether natural or legal person hold or control accounts, and to ensure that competent authorities have a process to identify assets without prior notification to the owner.

Criterion 31.1 – a) Art. 3(1) of the CCP provides as a general rule, that public authorities, higher territorial units, municipalities and other legal entities and natural persons are obliged to cooperate with LEAs (including prosecutors) and courts performing their duties relating to the criminal proceedings. While this cooperation generally extends to the provision of records and documents upon request, Art. 3(5) provides that information covered by banking, trade or tax secrecy, or information from the records of registered securities, may only be required by the court prior to the commencement of the criminal prosecution and by the public prosecutor in the preliminary investigation and, with its prior consent by the police officer, in the proceedings before the court by the presiding judge. Powers of the Police Force to obtain and to enforce the production of records and evidence related to ML, TF and large-scale financial crimes (including the production of data protected by banking secrecy) in the pre-investigative (operative) proceedings are provided for in Art. 29a of the Police Force Act.

b) The rules governing the search of persons and premises (house, land property etc.) as well as the entry into dwellings and other premises are provided under Art. 99 to 107 CCP in compliance with the respective FATF standards.

c) Competent authorities are empowered to take witness statements pursuant to Art. 131 to 139 CCP. In addition, Art. 127 CCP in line with the Constitution makes it a general obligation to appear at the summons of LEAs and the court and to testify as witness.

d) The CCP provides for detailed measures in this respect under Art. 91 (seizure of items) and Art. 90 for storing digital information as evidence (Storage and Disclosure of Computer Data) with further provision regarding the powers of the Police Force in the pre-investigative stage (Art. 21 of the PF Act).

Criterion 31.2 – The CCP provides for a wide range of investigative techniques mainly in Articles 108 to 118 with further provisions regulating the respective powers of the Police Force in applying such investigative measures in the operative (pre-investigative) stage of proceedings (Art 36 to 41a of the PF Act).

a) Undercover operations provided by the CCP (apart from those specifically referred to under C.31.2b to C.31.2d below) are the pretended transfer of things the possession of which is prohibited or it requires a special permit, as well as things that come from or which are intended to commit a criminal offence (Art. 112) covert surveillance of persons and items (Art. 113) preparation of video, audio or audio-visual recordings (Art. 114) and the use of undercover agents for the detection and investigation of certain offences (Art. 117). The measure under Art. 113 can generally be applied to all intentional criminal offences and those in Art. 112 and 114 to such offences punishable with at least 3 years of imprisonment as well as to corruption or other offences bound by an international treaty. The measure in Art. 117 is applicable to (serious) crimes (offences punishable by more than 5 years) and all forms of corruption, extremism, abuse of authority of a public official, and money laundering, as a result of which most potential predicate offences (including TF) are likely to be covered.

b) Interception and recording of telecommunications is provided by Art. 115 CCP. This special investigative measure is only applicable for a closed list of criminal offences in Art. 115(1) which however includes ML and (although not expressly) TF alike ("another intentional criminal offence, the performance of which is bound by an international treaty"). This wording makes it however likely that numerous predicate offences (those which are not expressly targeted by an international treaty) might not be suitable for interception.

c) Although the CCP provides for various measures by which computer data can be secured and stored for evidentiary purposes, or by which data on the performed telecommunication operations can be determined and reported, the AT have no information on any particular measure that would meet C.31.2(c).

d) Detailed rules of controlled delivery as a special investigative measure can be found in Art. 111 CCP. This measure is applicable to consignments that contain any of the illegal substances and objects listed in Art. 111(1) which also includes "items intended to commit a criminal offence or items of a committed criminal offence". This term is broad enough to encompass anything that is being smuggled or trafficked including cash or BNI. Powers of the Police Force in applying controlled delivery without initiating a criminal procedure are provided for by Art. 39 PF Act.

Criterion 31.3 – a) Establishing whether a natural or legal person holds or controls a banking account is only possible pursuant to Art. 3 paragraphs (1) and (5) CCP on the basis of which the LEA may request information covered by banking secrecy, with the consent of the public prosecutor, directly from the banks. There is no mechanism or specific legislation to provide for the timely execution of such requests, particularly as only requests written on paper form and sent

by ordinary mail are admissible according to the relevant legislation. No central register of bank accounts has yet been established in Slovakia.

b) The police have direct access to a number of relevant registers such as the vehicle records (EVO) and the real property register (KAPOR) as well as to public databases such as the Commercial Register (ORSR) vessel register, aircraft register, intellectual property, financial statements and the like No such query involves the prior notification of the natural or legal person involved.

Criterion 31.4 – Art. 26 (2)l of the AML Act requires the FIU to provide information to the Police Force for the performance of their tasks under a special regulation (in which context reference is given to Art. 2 of the PF Act which generally describe the tasks of the Police force). More specifically, Art. 26(3) of the AML Act read in conjunction with Art. 3(1) CCP expressly provides authority for state authorities acting for the protection of constitutional arrangement, internal order and security of the state for the fulfilment of their statutory tasks in the fight against terrorism and organised criminal activity (which practically includes LEA and prosecutors alike) to request all relevant information and document from the FIU.

Weighting and Conclusion

The Slovak Republic meets most of the requirements of Recommendation 30 and notwithstanding that law enforcement and investigative authorities have a broad range of powers to fulfil their duties, some of the special investigative techniques are not applicable to all potential predicate offences and accessing computer systems (i.e. a remote access to data stored in a computer system) does not seem to be provided for. Also, there is no central register of bank accounts in Slovakia and the existing mechanisms for identifying the holders or controllers of bank accounts does not ensure a timely performance. **R.31 is rated LC.**

Recommendation 32 – Cash Couriers

Slovakia was rated partially compliant with the former FATF SRIX. Apart from certain issues of effectiveness, the main technical downgrading factor was the inconsistency caused by the coexistence of two parallel cash reporting systems and forms (based on two different pieces of legislation).

Criterion 32.1 – Slovakia has established a declaration system for incoming and outgoing transportation of cash and BNIs across the external borders of the EU by physical persons. As at the time of the 4th round of MONEYVAL evaluations, the declaration regime is based on the EU Regulation (EC) 1889/2005 which is directly applicable in Slovakia as an EU Member State, but its provisions are underpinned by the provisions of the Customs Act (Act 199/2004 Coll.). In this regime, however, intra-Communitarian movements of cash or BNIs as well as transportation of cash or BNIs by legal persons or by use of mail or cargo (even across the EU external borders) are not considered as cross-border transportation and hence they are not subject to any declaration or disclosure obligation in Slovakia.

Criterion 32.2 – The declaration system mentioned under c.32.1 obliges any natural persons entering or leaving the territory of the EU carrying cash or BNIs in amounts equal to or greater than EUR 10,000. Passengers who meet this criterion are obliged to declare this fact in writing, by use of the reporting form prescribed by the Decree of the Ministry of Finance No. 161/2016 Coll. (Slovakian authorities have resolved the issues noted in the 4th round MER and now they also use the CDF forms similarly to most of the other EU Member States.)

Criterion 32.3 – This criterion is not applicable as Slovakia operates a declaration system.

Criterion 32.4 – Art. 4(2) of the Customs Act provides that the customs authorities exercise control of compliance with the reporting obligation, which includes the right to request the necessary assistance of the person subject to control and to making the person fill a correct CDF form including data as to the origin of the assets. In line with the wording of the directly applicable EU Regulation 1889/2005, no specific distinction is made between false declarations and failures to declare as provision of incorrect information in a declaration is considered to be a failure in itself.

Criterion 32.5 – Failure to comply with the reporting obligation under Art. 4 of the Customs Act is an administrative offence under Art. 72(1)(n) of the same Act. It is punishable either as a customs tort/delict (if committed by a legal person or a natural person entrepreneur) in which case it is sanctioned by a fine of up to EUR 99,581.75 or as a customs offence (if committed by a natural person) in which case the fine may go up to EUR 3,319.39 depending, in both cases, on the gravity of the infringement of customs rules (see Art. 74 and Art. 80[2]). Forfeiture of goods and articles is another possible sanction in both cases (see also C.32.11). In a so-called summary procedure, the maximum fine for natural persons is EUR 1,659.69 while in ticket procedure the maximum fine is reduced to EUR 331.93 which are far from being dissuasive.

Criterion 32.6 – As it was at the time of the previous assessment, the completed declaration forms as well as notifications on any infringements of the reporting obligation are submitted to the FIU but only on a monthly basis i.e. by the fifth day of the next calendar month (see Art.4[4] of the Customs Act).

Criterion 32.7 – Apart from the involvement of the Financial Administration in the ML-related multidisciplinary integrated group NES-LP within the MEKO, the AT were not provided with any example for an adequate co-ordination among customs, immigration and other related authorities on issues related to the implementation of Recommendation 32.

Criterion 32.8 – The existing legal framework does not authorize the Customs or other bodies to stop or restrain currency for a reasonable time in order to ascertain whether evidence of ML/FT may be found in cases mentioned under c.32.8. The Act on the Financial Administration (Act 35/2019) empowers the armed members of the Financial Administration (including Customs officers) to seize goods or things related to an infringement of customs regulations, tax regulations or other special regulations whereunder authorities of the Financial Administration perform their tasks and where necessary for the fact-finding, for a maximum term of 60 days (Art. 44). At the same time, the Customs Act (Art. 64) also provides, in a somewhat redundant manner, that Customs officers may seize goods or articles related to customs offences or customs torts/delicts (as instrumentalities, proceeds or evidence etc.). Even if cash/BNIs can be subject of these measures as *"things/articles"* neither of the provisions mentioned above could provide for seizing them solely for the purpose of ascertaining whether there is evidence of ML or TF.

Criterion 32.9 – The general requirement for exchange of information among EU countries and with third countries is regulated by Art. 6 and 7 of the EU Regulation 1889/2005. Slovakia also applies Council Regulation (EC) 515/97 on mutual administrative assistance in customs matters. International conventions (Naples II, Nairobi Convention) provide basis for international customs cooperation in non-EU relations while in the course of criminal proceedings, MLA may be sought and provided (see R37-R38).

The retention period of all related documentation (covering all three categories under C.32.9) by the Customs authorities is ten years.

Criterion 32.10 – Slovakia, as an EU Member State, applies the safeguards to the personal data privacy ensured by Art. 8 of the EU Regulation 1889/2005 and respects Preamble I of the same

Regulation which declares that the European Community endeavours to create a space without internal borders in which the free movement of goods, persons, services, and capital is ensured. EU Regulation 45/2001 on the data protection is also directly applicable in this context to the processing of personal data by all Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law.

Criterion 32.11 – In principle, natural persons transporting currency or BNI that is related to ML/FT or predicate offences would be subjects to the same criminal sanctions as referred under R.3 above, in which case the general confiscation and provisional measures regime would be applicable to the respective currency or BNIs. This is however seriously limited by the scope of the obligation to declare as discussed under C.32.1 and particularly the lack of Customs powers to stop or restrain currency so as to ascertain whether evidence of ML/FT may be found.

Weighting and Conclusion

Similarly to other EU Member States, Slovakia does not have an EU-internal border declaration system for cash or BNIs which deficiency has a general impact on the entire Recommendation. As for EU-external borders, there is no power to stop or restrain cash/BNIs for a reasonable period of time in order to ascertain whether evidence of ML/FT may be found. Transportation of cash/BNIs by legal persons and/or cross-border transportation of cash/BNIs via mail and cargo are not covered by the legislation. Sanctions for non-declaration or false declarations are not dissuasive enough. **R.32 is rated PC.**

Recommendation 33 – Statistics

Slovakia was rated PC for the former Recommendation 32 in the 4th round of evaluation Main factors where: Inconsistencies between the various data; statistics collected by the FIU did not focus sufficiently on ML and TF cases, but rather on general criminality; there were no statistics on international co-operation and requests for assistance from foreign supervisory authorities; no detailed and comprehensive statistics were from the MoF; no collective review of the Slovak system done at any level; no comprehensive and adequately detailed statistics on MLA were kept and maintained by the Slovak authorities both in general terms and specifically on ML/TF offences; no statistics on the NBS's and MoF's international co-operation on supervisory issues were kept.

Criterion 33.1 – According to Art. 27 (1) of the AML/CFT Act, the FIU shall keep a "summary" of statistical data covering the number of UTR and other reports received, follow-up given, the number of cases submitted to LEAs or tax administration. The number of persons prosecuted and convicted of ML as well as the value of seized and confiscated property shall also be maintained.

The GPO SR publishes yearly basic statistical data in the so-called *"Statistical overview of crime"*, which is available on the website of the GPO.

The NRA has identified statistical data quality as a permanent challenge and the authorities agreed that special attention has been paid to this aspect, especially when distinguishing qualitative and quantitative data.

a) FIU keeps statistics on UTRs, received and disseminated, according to Art. 27 (1) of the AML/CFT Act as described above.

b) The FIU registers in the electronic information system (DMS), data on the number of UTRs under investigation which triggered investigations and prosecution decisions up to the level of the court. An example of such statistical overview was presented as an amendment to the FIU Annual Report for 2017. At LEA level, the statistics on ML investigations are incomplete or not kept. The

Automatic Information System of the GPO contains all the basic information regarding the quantitative data at the prosecutions stage.

c) The GPO keeps statistics on frozen and seized property but there are no statistics on confiscations. The statistics kept do not differentiate between proceeds, instrumentalities and property of equivalent value. The absence of comprehensive and detailed statistics posed an unsurmountable impediment to assessing the performance and effectiveness of the confiscation regime and the actual recovery of confiscated assets (see also IO8).

d) Basic statistical indicators concerning all forms of passive and active judicial cooperation in criminal cases are part of the Public Prosecutor's Office's PTCA system. All received and sent requests from/to are kept by the FACO and the Customs Department Financial Directorate in an application superstructure of financial administration under the name OIS – requests. The FIU keeps statistics on incoming and outgoing international requests for co-operation.

Weighting and Conclusion

Significant steps have been undertaken by the authorities to improve statistics. There is provision in AML/CFT Act that makes obligation to FIU to keep comprehensive statistics. Similar requirements have been introduced at the Prosecutorial level. However, there are no statistics on the ML and TF investigations, the statistics kept on seizures, confiscations and assets recovered are deficient. **R.33 is rated PC.**

Recommendation 34 – Guidance and feedback

In the 2011 MER, Slovakia was rated PC with the previous R.25. The report noted the unsatisfactory co-operation with the DNFBP; absence of specific guidance for some of the RE; feedback provided to RE not always substantive and descriptive enough; and insufficiently developed case-by-case feedback.

Criterion 34.1 – *Guidelines*

According to Presidium of Police force Instruction 6/2019, the FIU shall develop and issue methodological materials and guidelines for obliged entities in order to raise legal awareness in the area of competence of the reporting agent. The FIU issued notices (opinions) and Guidelines in the interpretation and application of the AML/CFT Act which are published on the website. FIU submits opinions only based on a written request of a specific obliged entity, whose conditions are specified on the FIU website. The Guidelines, which are also publicly available on the FIU website, are general and concern the interpretation and practical application of selected provisions of the AML Act concerning all obliged entities. Also, the FIU publishes on its website the Annual Reports for the previous period as well as a NRA public report, from which obliged entities can obtain information on risks and trends in AML/CTF developments.

The FIU has published 11 guidelines on its website, one relates to life insurance contracts, three relate to DNFBPs, and seven relate to the enforcement of the law by all categories of obligated entities on issues such as UT reporting, KYC, data processing etc... Nevertheless, important aspects of the AML/CFT regime are not covered by the Guidelines such as guidance on the application of CDD requirements.

Feedback

Art. 26 (i) of the AML/CFT Act stipulates that the FIU shall inform the obliged entity on the efficiency of unusual transaction reporting and on the procedures that follow the receipt of unusual transaction report unless there is a threat of hampering the processing of the unusual

transaction. Nevertheless, from the text of the Act it appears that the provision is of a general nature and refers to the procedure that the FIU shall adopt after the receipt of URTs rather than a form of specific feedback on the quality of the UTRs and the manner in which they have been used by the FIU. FIU submits opinions (as a form of feed-back) based on a written request of a specific obliged entity, whose conditions are specified on the FIU website.

Weighting and Conclusion

The Slovak Republic has a minor shortcoming in that the Guidelines already published are not covering all the REs and all the AML/CFT areas. Also, the legal provisions related to feedback are rather general. **R.34 is rated LC.**

Recommendation 35 – Sanctions

In the 4th round previous MER, Slovak Republic was rated as PC with the previous R.17. There were no clear provisions to avoid double sanctioning by the FIU and other supervisors. The FIU also could not apply sanctions to directors and senior management of obliged entities. The FATF standards were revised since then and the new analysis has been undertaken.

Criterion 35.1 –

Recommendations 8-23

The FIU may sanction all obliged entities for failing to comply with any of the duties laid down in the AML/CFT Act (Art. 33(1)). The sanctions however cannot be applied to natural persons such as their directors and other senior executives. Other supervisory authorities (NBS & MoF) are required to inform the FIU once they uncover violations of AML/CF requirements as part of their inspections (Art. 29(5)).

In determining the type/amount of the sanction (either a fine or other administrative sanctions), the FIU takes into account the seriousness, duration and consequences of the violation, as well as well as the level of cooperation provided by and size of the obliged entity, and whether the violation has been committed repeatedly (Art. 33(4)).

Furthermore, if the obliged person violates the provisions of the AML/CFT Act consecutively for 12 months or repeatedly, the FIU has powers to request the relevant supervisory authority - either the NBS or MoF (GRA) - to withdraw the authorization (license) (Art. 34). The supervisory authority in question is obliged to inform the FIU about the follow-up action taken within 30 days. The authorities stated that the NBS shall take into account the severity, duration and consequences of uncovered violations when considering the FIU's request to withdraw the authorization (license) of banks and securities market intermediaries (Art. 50(1) of the Law on Banks). The authorities did not explain the legal processes for withdrawing, restricting or suspending the authorization (license) of other obliged entities for AML/CFT violations. The authorities did not explain the precise legal processes/mechanisms for withdrawing, restricting or suspending the authorization (license) upon the FIU's request.

The FIU may impose fines of up to EUR 5,000,000 with regard to banks and other FIs and up to EUR 1,000,000 with regard to DNFBPs for violations concerning CDD and EDD measures (PEPs, correspondent banking), record-keeping, reporting and suspension of unusual transactions, submission of data to the FIU, and prohibition on dealing with shell banks (Art. 33(1)). The FIU may also impose fines of up to EUR 200,000 for any other violation of the AML/CFT Act (Art. 33(3)), issue cease and desist orders (Art. 33(6)), and require the publication of the FIU's decision to impose a sanction unless this would endanger the stability of the financial market (Art. 33a(1)).

The time limit for imposing sanctions is five years from the day when the violation occurred (Art. 33(5)).

The NBS may impose a fine of up to EUR 300,000 (or in case of repeated or severe violations, up to EUR 600,000) for the provision of unauthorized payment services or for breaches of information requirements concerning wire transfers under the Law on Payment Services (No. Art. 78(2) & Art. 86(2) (see also R.14).

The authorities did not explain what are the sanctions for breaches of information requirements concerning wire transfers that are not part of the AML/CFT Act.

Recommendation 6

The sanctions for the violation of requirements concerning terrorism & terrorist financing related TFS are provided by the Law on Implementation of International Sanctions (No. 289/2016). In particular, Articles 21 and 22 stipulate that breaching a restriction, order or prohibition ensuing from an international sanction, or a failure to report the identified property subject to freezing measures shall incur a fine from EUR 5,000 to EUR 66,400, while breaching the tipping-off prohibition therein shall result in a fine from EUR 109 to EUR 6,600. Where these violations result in jeopardizing foreign policy and security interests of Slovak Republic, the amount of fines may double, and where they also result in a benefit for the person concerned or a damage exceeding EUR 16,600, a fine from EUR 132,800 to EUR 1,659,700 can be imposed. The authorities did not explain which state authority if responsible for applying the penalties and what are the criteria for determining the amount of fines that is proportionate to the violation.

The financial sector

The Supervisory bodies under the Gambling Act (article 54) have powers to impose sanctions for the entities under their supervision if there are identified violations of the gambling act, special acts and other generally binding legal regulations applicable to gambling game operation, promotion of gambling games, conditions of operation of gambling games laid down in this Act or specified in an individual license or general license, the duties according to the approved game plan including the gambling game rules or fails to fulfil the duties imposed upon them by a valid decision of the supervisory body. The supervisory body imposes the sanctions on the nature, seriousness, way, rate of guilt, length of duration and consequences of the violation of duties.

The measures applied to banks for not complying with the legal framework are provided by article 50 of the banks act:

"(1) Where NBS finds any shortcomings in the operations of a bank or a foreign bank branch consisting in a failure to comply with the terms and conditions stipulated in its banking authorisation or in a decision on prior approval, or with the requirements and obligations specified in other decisions of NBS imposed on a bank or a foreign bank branch, a failure to meet the conditions stipulated in Article 7(2), (4) and (6), and Article 8(2), (4) and (6), or a violation or circumvention of other provisions of this Act, legally binding acts of the European Union pertaining to banking activities, separate regulations,46 or other legislation of general application governing the conduct of banking operations, NBS may, depending on the seriousness, scope, duration, consequences, and nature of detected shortcomings" apply remedial measures, penalties or impose fines based on the impact determined by the fail of compliance.

The NBS has also enforcement and corrective measures regarding the other participants in the financial market as follows:

- article 144 of the Act no 566/2001 on securities and investment practices provides corrective measures and fines to be imposed for noncompliance with the provisions of the act and separate laws;

- article 139 of the Act no 39/2015 on insurance provides sanctions for noncompliance with the legal provisions of this Act and other separate laws;

- article 78 (2) of the Act no 492/2009 on payment services provides corrective measures for not complying with the provisions of the mentioned act and other separate law and regulations;

- article 24a of the Act no 202/1995 on foreign exchange provides corrective measures for failing to comply with the provisions of the abovementioned act.

The entire financial market legal framework, respectively all the regulations abovementioned use the same wording. Looking at the article 50 of the bank act written above, it seems that this provision could also be used for not complying with any of the AML obligations but it's not specific for AML obligation. It is not enough to make references to other special regulations or other legally binding acts. AML breaches should be regulated in a special act and provide also specific sanctions for not complying with Recommendations 6, 8 to 23.

The DNFBPS

The AML Act provides sanctions for AML breaches of the DNFBPs and SRB can withdraw certificates/license if any of the conditions on which it were issued are no longer available. There are no special regulations to impose AML sanctions for natural and legal persons (DNFBPs).

Criterion 35.2 – Sanctions for AML/CFT violations do not apply to directors of obliged entities and other senior management.

Sanctions for directors and senior management

According article 18 of the AML Act, the administrative sanctions to natural persons can be applied only for violation of the obligation of confidentiality.

The financial sectors' supervisor has powers to impose a fine up to EUR 5,000,000 to a member of a bank's management, a chief executive officer, a senior employee (article 50 of the Act of banks). The insurance sector has in place measures to impose to members of the board of directors or supervisory board, to the head of a branch, or any other natural person controlling an insurance or a reinsurance undertaking a fine up to 50% of twelve times the monthly average of their income (article 139 (6) of the Act of insurance). The securities sector has in place measures imposing a fine up to twelve times the monthly average of the income of a director or a senior manager (article 202 (2) of the Act of securities). NBS can also impose sanction to a natural person who holds the position of a statutory body or member of the statutory body or supervisory body of a financial agent or a financial adviser, respectively a fine up to EUR 50,000 (article 39 (7) of the Act no 186/2009 on financial intermediation and financial advisory services). Although the country presented a range of sanctions for directors and other management functions of the financial sector, there are no sanctions for the management functions of the DNFBPs.

Weighting and Conclusion

No sanctions can be imposed on senior management of obliged entities. The sanctions available for violations of terrorism & terrorism financing related TFS are not proportionate and dissuasive. **R.35 is rated PC.**

Recommendation 36 – International instruments

In its 2011 MER SR was rated as PC with the former R.35. In addition to concerns over effectiveness, treated elsewhere in this evaluation, the factors contributing to this rating were as follows: 1) Reservations about certain aspects of the implementation of the Vienna, Palermo and TF Conventions, and 2) that the financing of some of the acts defined in the treaties appearing in the Annex to the TF Convention had not been criminalised as TF offences. The latter factor also contributed to the rating of PC for SR I. The remaining identified deficiencies related to the implementation of certain UNSC Resolutions – an area that is no longer within the scope of new R.36.

Criterion 36.1 – The SR is a party to the Vienna Convention, the Palermo Convention, the Merida Convention and the TF Convention. None of the above have been subject to reservations. For the sake of completeness, it should be noted that it is also a party to all of the instruments listed in the Annex to the TF Convention.

R36 also encourages states to ratify and implement other relevant international conventions including the Council of Europe Convention on Cybercrime, 2001 and the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, 2005. While not subject to assessment under the FATF Methodology the evaluators note that the SR is a party to both of these instruments.

Criterion 36.2 – The Slovak authorities provided a table detailing the manner in which the SR has implemented the complex and numerous provisions of the four UN Conventions addressed by the FATF methodology.

On this basis it can be concluded that, generally speaking, the requirements of this criterion have been satisfied. As seen in the earlier analysis of R3 (money laundering) and R5 (terrorist financing) minor deficiencies with regard to the implementation remain.

Weighting and Conclusion

While the SR has become a party to the Vienna, Palermo, Merida and TF Conventions certain deficiencies have been identified in their implementation into domestic law. **R.36 is rated LC.**

Recommendation 37 - Mutual legal assistance

In the 4th round of MONEYVAL evaluation, Slovakia was rated Largely Compliant for both the then R.36 (MLA) and R.37 (dual criminality). The downgrading factors for both Recommendations were the limitations in the criminalization of the TF that might limit the ability of Slovakia to provide MLA and, for R.36, an additional factor of effectiveness.

Criterion 37.1 – In the field of international legal cooperation, international treaties and binding EU legislation enjoy precedence over national laws by virtue of the Constitution of the Slovak Republic (Art. 7) and hence the domestic legislation applies only if such international/EU instruments do not regulate otherwise (Art. 478 CCP). Slovakia is a party to all major UN and CoE Conventions in this field and, for the relations with EU Member States, it implemented all EU legislation concerning MLA in criminal matters the latest being the European Investigation Order (EIO) as provided by the Law on EIO (Coll. 236/2017).

As for the domestic legislation, the provision of MLA is provided by Part V Chapter V of the CCP (with general provisions in Chapter I) and it encompasses every action performed in the territory of Slovakia upon a letter rogatory of a foreign authority, in particular the serving of documents, interrogation of persons, and performance of any other evidentiary acts provided for by the CCP.

The widest possible range of MLA can therefore be provided for all criminal offences referred to in C.37.1.

As far as MLA provided to EU Member States is concerned, the Law on EIO provides for strict deadlines for executing such a request, in line with the underlying EU legislation (30/60 days) in addition to which the EUROJUST is also available for facilitating rapid communication of EIOs and the evidence requested. For non-EU foreign requests, there are no CCP or other legal provisions to set concrete deadlines for, or to specifically prescribe the rapid provision of MLA, but there are CCP articles that indirectly serve this purpose such as Art. 483 which makes it possible that the Slovakian authorities commence the execution of a foreign request if it has only arrived by fax or electronic means if there is no doubt about its reliability and if the matter cannot be deferred or Art. 484 which allows for sending and receiving requests and information through the INTERPOL and, for states that use the Schengen Information System, through SIRENE channels. Similar mechanisms are available under the European Convention on MLA and its Second Additional Protocol (see also the declaration made by Slovakia). As for the court procedures, the courts are obliged to provide MLA without undue delay pursuant to Decree of MoJ No. 543/2005 as amended.

Criterion 37.2 – In case the applicable international treaty or the implemented EU legislation do not provide otherwise, the mechanism established by Art. 538 CCP is to be applied, according to which foreign letters rogatory are received by the Ministry of Justice as the central authority. The Ministry then sends it to the district prosecutor's office having territorial competence to perform the requested act of legal assistance or, if such acts belong to the jurisdiction of more than one prosecutor's offices, to the Prosecutor General's Office for a decision as to which of them shall execute the request. If the subject of the request is solely an act to be performed by a court, the Ministry sends it directly to the competent court.

While the CCP mechanism does not provide for the direct communication of MLA requests, it is possible under various international and EU legal instruments. International legal cooperation between EU Member States (including the use of EIO) generally takes place between the competent judicial authorities which, in case of Slovakia, means the competent district prosecutor's office. The same goes for receiving and executing letters rogatory on the basis of the 1959 European Convention on MLA as amended by its Second Additional Protocol, while countries only bound by the European Convention may send their requests to the GPO (see the respective declaration made by Slovakia).

The Prosecution Service uses an IT case management system called PTCA that allows monitoring and controlling of the execution of incoming requests while there is a similar CMS established in the Ministry of Justice (Fabasoft) for managing incoming MLA requests. Within the latter, the progress on the execution of an MLA request is usually checked every 3 months unless a more frequent monitoring is requested by the other country.

Criterion 37.3 – The Slovakian legislation does not provide for specific grounds for refusing or restricting mutual legal assistance apart from the grounds provided for by the respective international treaties or other legal instruments. The only conditions in this field are that foreign requests may not be granted if their execution would violate the Constitution or any provisions of the Slovakian legal system or it would damage other important state interests (Art. 481 CCP) and that performing seizure of property and cross-border surveillance both require treaty basis (Art. 544 and 551 CCP) Neither of these conditions is unreasonable or unduly restrictive.

Criterion 37.4 – The Slovakian law does not allow for refusing a foreign request for mutual legal assistance on the grounds mentioned in subpara (a) and (b) of Criterion 37.4.

Criterion 37.5 – Art. 482 (1) CCP provides that Art. 6 CCP on the provision of information on criminal proceedings is equally applicable in international cooperation. These rules ensure that no information provided to the public will obstruct or hinder the clarification and investigation of the case. Specifically, Art. 482(2) provides that the Slovak authorities shall not disclose or provide any further information or evidence obtained from a foreign authority in relation to MLA, nor will they use them for purposes other than that for which they were sent or requested, if so requested by the respective foreign authority or so prescribed by an international treaty.

Criterion 37.6 – In cases that do not involve coercive measures (e.g. service or provision of documents, hearing of a witness or defendant, provision of banking evidence etc.) dual criminality is not a precondition for rendering MLA.

Criterion 37.7 – Dual criminality is only required for MLA involving coercive measures, that is, for any procedural act the performance of which requires a court order according to the provisions of the CCP (see Art. 539). In case a foreign letter rogatory is aimed at a procedural act that requires a court order, Art. 537 (3) CCP requires that the act concerned by foreign request is a criminal offence both in the Slovakian law and that of the requesting state. The wording of this provision makes it clear that the offence itself and not its denomination or categorization is to be considered.

Criterion 37.8 – As mentioned above under C.37.1 the Slovakian authorities can provide a wide range of investigative assistance to the requesting countries, which in principle extends to all powers and investigative techniques required under R.31 that are available domestically (provided that the foreign request complies with the conditions set by relevant international treaties or EU instruments).

All of the specific powers discussed under R.31 are available, on the same conditions as domestically, for the execution of a foreign MLA request. In case of EU legal instruments, provision is assistance is further facilitated by the principle of mutual recognition.

Weighting and Conclusion

All requirements are met. **R.37 is rated C.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

Slovakia was rated Partially Compliant for R.38 in the 2011 MER. The technical deficiencies identified in the 4th round included the limitations in the criminalization of the TF as well as the difficulties in forfeiting property from third parties which might equally limit the ability of Slovakia to provide MLA and the lack of concrete arrangements for co-ordination of seizure and confiscation actions with other countries or for sharing confiscated assets with them (apart from EU Member States covered by the respective Framework Decision).

Criterion 38.1 – The situation is largely the same as at the time of the 4th round of MONEYVAL evaluation. Requests from EU Member States for freezing or seizing property that can be subject of confiscation are executed on the basis of Act no. 650/2005 Coll. on the execution of orders to freeze property or evidence in the EU (implementing Council Framework Decision 2003/577/JHA) in which respect Art. 550-551 CCP serve as underlying domestic legislation (lex generalis). Foreign confiscation orders are recognized and executed pursuant to Act 316/2016 Coll. on the recognition and enforcement of property-related decisions issued in criminal proceedings in the EU (implementing Council Framework Decision 2006/783/JHA on the application of the principle of mutual recognition to confiscation orders) which instruments also provide for appropriate deadlines.

Confiscation orders issued by non-EU countries can be executed according to the CCP provisions dealing with the recognition and enforcement of foreign court decisions (Art. 515[2]e CCP) provided that there is a bilateral or multilateral treaty basis (Art. 516[1] CCP) such as the Warsaw or Palermo Conventions. Confiscation requires prior recognition of the foreign judgment by a domestic court order. There are no specific rules to provide for the expeditious enforcement of a foreign confiscation order. For the identification of assets subject to confiscation based on a foreign MLA request (regardless whether or not it comes from an EU country) all measures available in similar domestic cases are available.

Seizure of assets upon the request of a non-EU country is regulated by Art. 551 CCP as a specific form of MLA extending to all sorts of property under C.38.1 except for C.38.1(a) (see C.4.1[a] on laundered property). This measure requires a domestic court order based on a motion of the public prosecutor who, in urgent cases, may however issue a preliminary order which is subject to subsequent confirmation by the court.

Criterion 38.2 – Slovakian authorities can provide assistance to requests for cooperation made on the basis of non–conviction based confiscation proceedings and related provisional measures provided that such requests relate to instrumentalities of or proceeds from a criminal offence (considering that confiscation of a thing under Art. 83 CC is an *in rem* confiscation measure in itself, roughly in line with the scope of C.38.2). EU and domestic instruments mentioned under C.38.1 are equally applicable to foreign requests aimed at recognising and enforcing non-conviction based confiscation orders (as a minimum, if such orders are compatible with the measure under Art. 83 CC).

Criterion 38.3 – The Slovak authorities have had ad hoc arrangements for coordinating actions aimed at seizure and confiscation with other countries, mainly with EU Member States in which context the EUROJUST was used as a platform for coordination. Reference was made to a case example where coordination with Italian authorities under the auspice of the EUROJUST led to the seizure of 2 million EUR in Slovakia that constituted proceeds of carousel fraud having been investigated in Italy. (Recognition of a subsequent Italian confiscation order and sharing of the confiscated assets was under way at the time of the onsite visit.).

While there are mechanisms in place to manage and dispose seized and forfeited assets, these do not fully meet C.38.3(b) when it comes to active management of property or property items beyond safekeeping measures (see the analysis under C.4.4).

Criterion 38.4 – Sharing of confiscated property with EU Member States is provided for by virtue of the aforementioned Act 316/2016 Coll. (see C.38.1). Slovakian authorities claim that in case of non-EU countries, the procedure is the same as described under 38.1 in relation to the recognition and enforcement of foreign confiscation orders. The respective CCP articles, however, do not contain any direct provision on sharing of confiscated assets, apart from Art. 517[3] stipulating that the court must decide to which country the property that is subject of the foreign confiscation order shall belong, which is, as a main rule, the Slovak Republic unless the court decides otherwise – which implies that asset sharing is not excluded by law, but not expressly provided for either. It would also require a clear treaty basis, but the assessors have no information on any existing arrangement in this field (similarly to the findings of the previous MER).

Weighting and Conclusion

Slovakia is generally able to respond to foreign requests countries to identify, freeze, seize, or confiscate, but the mechanism for enforcing non-EU confiscation orders does not allow for an expeditious action. The mechanisms in place for managing, and when necessary disposing of,

property frozen, seized or confiscated suffer from certain deficiencies described under R.4 and sharing of confiscated assets with non-EU countries is only implicitly regulated by law and is not addressed by any existing arrangement. **R.38 is rated LC.**

Recommendation 39 – Extradition

The last time Slovakia was evaluated against R.39 was in the context of the 3rd round MER in 2006 when this Recommendation was rated Largely Compliant for reasons of effectiveness (in the absence of statistics, it was not possible to determine whether extradition requests had been handled without undue delay.)

Criterion 39.1 – Extradition to foreign non-EU states is primarily regulated by the relevant international treaties (such as the 1957 European Convention etc.) but it is also possible on the basis of reciprocity. Definition of extraditable offences and detailed procedural rules can be found in Art. 498-514 CCP. Surrender to EU Member States based on a European Arrest Warrant is regulated by Act No. 154/2010 Coll. on the EAW (hereinafter: Law on EAW) which implemented the respective Council Framework Decision.

a) According to the CC of Slovakia, both ML and TF are criminal offences punishable with more than one year of imprisonment (see R.3 and R.5) and therefore both are extraditable offences pursuant to Art. 499(1) CCP as well as Art. 4 of the Law on EAW. No deficiencies in the criminalization of ML or TF appear to pose any notable impediment to international cooperation in this field.

b) The EAW proceedings are determined by strict deadlines for the execution of a EAW which in itself guarantees timeliness of the procedure. No such conditions apply however to extradition to non-EU countries. It is unclear whether and which legal provisions would ensure clear processes for the timely execution of extradition requests. Extradition cases are part of the case management systems run by the Prosecution Service (PTCA) and the Ministry of Justice (Fabasoft) mentioned above under R.37.

c) The grounds for refusal of extradition to non-EU states are stipulated in Art. 501 CCP (grounds for inadmissibility) with further provisions in Art. 510(2) (grounds for ministerial non-authorization even if the extradition would otherwise be admissible) neither of which can be considered unreasonable or unduly restrictive. Refusal of a EAW from a EU Member State is allowed in an even more limited scope (see implemented by Art. 23 of the Law on EAW.

Criterion 39.2 – a) As a general rule, the extradition of Slovakian citizens to a foreign (non-EU) country is inadmissible unless it is specifically provided by law, an international treaty, or the decision of an international organisation by which the Slovak Republic is bound. To date, there are no such treaties except the Rome Statute of the International Criminal Court. Surrender of Slovakian nationals to other EU Member States is however possible by means of a European Arrest Warrant (Art. 23[4] of the Law on EAW).

b) Pursuant to Art. 510(3) CCP, if the Minister of Justice does not authorise the extradition for any reason (including the grounds of nationality) the said Ministry shall submit the matter to the General Public Prosecution for a criminal prosecution in compliance with the legal system of the Slovak Republic. In such cases, deciding on initiating domestic criminal proceedings is based on an evaluation like in cases of taking over criminal proceedings from abroad and indeed, the Slovak Republic would normally consider requesting the transfer of proceedings in such cases.

Criterion 39.3 – As a general rule, dual criminality is required for extradition. Art. 501 para (d) CCP provides that extradition is inadmissible if the act for which the extradition is requested is

only a criminal offence under the legal system of the requesting state, but not under the legal system of the Slovak Republic. The wording of this provision makes it clear that the offence itself and not its denomination or categorization is to be considered, which interpretation is underpinned by Supreme Court jurisprudence (No. 2Urto 1/2016). A similar mechanism applies for EU Member States in surrender proceedings based on a EAW (see implemented by Art. 4[2] of the Law on EAW). No double criminality condition applies, however, to 32 categories of serious offences (listed in Art. 4[4] including ML) if they are punishable under the laws of the issuing Member State by imprisonment for more than three years.

Criterion 39.4 – Procedures for simplified extradition are in place both for non-EU countries (see simplified extradition proceedings in Art. 503 CCP) and for EU Member States (see simplified surrender proceedings as implemented by Art. 24[1] of the Law on EAW).

Weighting and Conclusion

Slovakia meets most of the criteria under Recommendation 39. Although the legal framework that regulates extradition and surrender mechanisms are generally in line with the FATF standards, there are no clear processes for the timely execution of extradition requests issued not in the form of an EAW. **R.39 is rated LC.**

Recommendation 40 – Other forms of international cooperation

Slovakia was rated LC for Recommendation 40 in the fourth round. The reservations were related to lack of detailed statistics which has been undermining the assessment of effectiveness.

Criterion 40.1 – The Slovak legislation envisages grounds for providing international assistance among competent authorities in relation to ML, associated predicate offences and TF, particularly in the AML/CFT Act. The legal assistance is usually provided upon request but exchange of information is also spontaneously possible. In case of the FIU the cooperation differs on political basis (EU membership) as described under EC40.11 below. The timelines for FIU international cooperation with other FIUs is set in Article 6 (3) of the Order of FIU Director on Method of Implementation of an International Exchange of Information: three days for urgent requests and 30 days for other requests.

Criterion 40.2 – The competent authorities have an extensive legal basis for international cooperation (Art. 26 (1) and Art. 28 of the AML/CFT Act, Article 77a of the PF Act, Art. 1 (3) (h) of the Financial Market Supervision Act, Art. 1 (3) of the Act on SIS, Act No. 359/2015 Coll. on the Automatic Exchange of Financial Account Information for the Tax Administration Purposes, Act No. 442/2012 on international assistance and cooperation in tax administration). No particular impediments exist with regard to the means available for execution of international cooperation requests. The authorities use clear and secure gateways, such as the Egmont Secure Web for international exchange of information; diplomatic channels; Interpol; Europol and SIRENE. The safeguards on confidentiality of information are incorporated in the AML/CFT Act (Art. 18). Nevertheless, there are no mechanisms or rules for the prioritisation and timely execution of the requests, except for situations provided under 40.1.

Criterion 40.3 – In some instances, the competent authorities can cooperate in the absence of agreements. Nevertheless, if a foreign partner requires an agreement to perform its international cooperation, the FIU will sign a Memorandum of Understanding with it upon request. Since its establishment, the FIU has concluded 8 Memoranda of Understanding (with the FIU Belgium, FIU Czech Republic, FIU Poland, FIU Ukraine, FIU Monaco, FIU Australia, FIU Albania, FIU Russian Federation). For the NBS and PF a memorandum (which is concluded pursuant to Section 51 of Act

No. 40/1964 Coll. Civil Code, as amended on the basis of § 34a par. 2 of the Act of the National Council of the Slovak Republic No. 566/1992 Coll. on the National Bank of Slovakia, as amended and § 77b para 1, letter a) and § 77c para 1 of the Act on Police Corps) is required only in case of performing supervisory actions/police activities on the territory of a foreign state.

A Multilateral Agreement on the practical modalities for exchange of information on AML/CFT under Art. 57a (2) of Directive (EU) 2018/843, was signed between the ECB, the NBS, and the FIU on 10 January 2019. If cross-border cooperation is required, cooperation agreements with other Member States are concluded with the respective authorities. Slovakia has concluded bilateral agreements with neighbouring countries[68].

There are no provisions regarding the timeliness for the negotiation and signature of the agreements in cases where those are required.

Criterion 40.4 – Upon request, ARO provides feedback on the use and usefulness of the information obtained through CARIN network. Police authorities provide the competent authorities with information on the use and usefulness of the information sent to them, within the limits of the legal system of the SR based on the Council Framework Decision No. 2006/960 / JHA. However, this does not apply to Non-EEA countries. Provision of feedback by the Slovak FIU is regulated in Section 5 (2), (f) Order of FIU Director on Method of Implementation of the International Exchange of Information. NCB Interpol is bound by the terms of providing the responses to the supplementary information exchange by the Interpol Constitution and rules of data proceeding. National SIRENE Bureau is bound by the terms of providing the responses to the supplementary information exchange by the SIRENE Manual.

Criterion 40.5 – There are various circumstances in which a request for assistance may be refused, but those do not relate to fiscal matters, or secrecy or confidentiality of financial institutions or DNFBPs. The nature or status of the requesting counterpart authority is not relevant for international cooperation. Exceptions are possible but are not inconsistent with the requests of this criterion. The PF may refuse to provide or disclose information or personal data if it would jeopardize the safety of persons, would damage basic interests of the SR, would jeopardize the success of the on-going detection, clarification, investigation, prosecution or enforcement of a decision in criminal proceedings.

Criterion 40.6 – The information provided by the FIU to foreign authorities may be used only for the purposes defined and with the prior consent on the handling of the information. Similarly, the information provided by the foreign authorities to the FIU may be used only for the purposes defined and with the prior consent on the handling of the information, on the basis of EGMONT Group principles.

According to Act No 747/2004 of 2 December 2004 on financial market supervision and on the basis of bilateral agreements (e.g. Memorandum of Understanding IAIS, Sienna Protocol) the NBS

[68] Agreement between the SR and the Republic of Poland on cooperation in the fight against crime and cooperation in border areas; Agreement between the SR and the Republic of Hungary on Cooperation in Preventing Cross-border Crime and in the Fight against Organized Crime; Agreement between the SR and the Republic of Austria on Police Cooperation, Agreement between the SR and the Czech Republic on cooperation in the fight against crime, in the protection of public order and in the protection of the state border.

may make available or provide information to other authorities or persons, or otherwise disclose it, only with the consent of the foreign supervisory authority that provided the information.

According to Art. 482 (2) of the CCP, the Slovak authorities shall neither make public nor forward information or evidence received from a foreign authority on the basis or in connection with a request received or made under this Chapter, nor shall they use it for purpose other than that for which it was provided or requested if an international treaty contains an obligation to this effect or if the foreign authority provided the information or evidence only under the condition of compliance with such restrictions; this restriction shall not be applied if the foreign authority gives its consent to making the information or evidence public or to using it for a different purpose. The Europol Regulation, Interpol Constitution and Schengen acquis provide for the exact purpose of the use of the information and the obligation to handle it as determined by the applicant.

Criterion 40.7 – The level of protection of information obtained in the framework of international cooperation is identical to the level of information obtained at national level by established rules, principles and technical means. The confidentiality of information for FIU is defined in Art. 26 (1) (g) of the AML/CFT Act. Pursuant to par. 9 of the Police Act, the PF may provide or make available personal data to an international body or a third State which does not guarantee an adequate level of protection if it provides other appropriate safeguards or it is in the interest of the person concerned or because of another important public interest. The distribution of information to competent authorities is ensured by adequate encrypted communication methods based on mutual agreement with specified procedures and technical means. Police officers providing the information exchange are bound by the obligation to safeguard the information which is exchanged and to respect principles of personal data protection.

Criterion 40.8 – Art 28 of the AML/CFT Act has a broad wording which states that the FIU cooperates with the bodies of other countries within the scope and under the conditions laid down in the international treaty binding the Slovak Republic or on the basis of non-contractual reciprocity principle. The authorities interpret this provision as the FIU is authorized to exchange all available information at the request of a foreign FIU, and can obtain information on their behalf. When it comes to accessing information and databases, it makes no difference whether the FIU conducts its own analysis or acts upon a foreign request. ARO does not apply stricter conditions than those imposed by national law in the provision of information and intelligence to competent law enforcement authorities of other EU Member States and non-EU Member States, which apply at national level in providing information to law enforcement authorities proceedings in the Slovak Republic. No information was provided regarding the NBS and Police Forces.

Criterion 40.9 – The FIU has a legal basis for cooperation with foreign partners as set out in Art. 28 of the AML/CFT Act, regardless of whether their counterparts FIUs are administrative, law enforcement, judicial or other nature. The differentiation between FIUs is done on other criteria as explained under EC40.11.

Criterion 40.10 – The FIU provides feed-back to their foreign counter-parts, upon request based on Section 5 (2) (f) of the Order of FIU Director on Method of Implementation of the International Exchange of Information.

Criterion 40.11 – The FIU's international cooperation is governed by Art. 28 of the AML/CFT Act which stipulates two categories of counter-part FIUs: the EU countries FIUs (Art. 28 (1)) and the rest of the FIUs (Art. 28 (2)). While in the first case the Slovak FIU shall cooperate with the competent bodies in exchanging and verifying the information necessary for money laundering and terrorist financing without any condition, the second paragraph is more restrictive, and limits

the cooperation *"within the scope and under the conditions laid down in the international treaty binding the Slovak Republic or on the basis of non-contractual reciprocity principle"*. Therefore, the extensive direct or indirect information exchange with non-EU FIUs is subject to conditions laid down in each particular treaty. That being said, no impediments have been reported in practice.

Criterion 40.12 **–** According to Articles 1(3)(h) and 3(3)(7) of the Law on Financial Market Supervision, the NBS is authorized to cooperate with both EEA and third country financial market supervisory authorities by sharing information for supervisory purposes. When the NBS is requested to divulge confidential information, this can be done by concluding cooperation and information-exchange agreements with foreign counterparts. The authorities did not provide information if any such agreements have been negotiated and/or concluded with third country supervisors. FIU can also exchange information obtained in its supervisory capacity with foreign counterparts with the limitations described under EC40.11.

Criterion 40.13 **–** As noted above, the NBS can exchange information with its foreign counterparts. The applicable legal provisions do not contain any limitation as to what type of information can be shared. Such details must be spelled out in the cooperation and information-exchange agreements under Article 3(7) of the Law on Financial Market Supervision. More detailed provisions on the exchange of information held by FIs, with a particular focus on EEA supervisory authorities, is provided in the relevant pieces of sectorial legislation. FIU can also exchange information obtained in its supervisory capacity with foreign counterparts with the limitations described under c40.11.

Criterion 40.14 **–** The scope of information that the NBS is able to exchange internationally (subject to conditions described in c.40.12 and c.40.13) is not restricted and can therefore include regulatory, prudential and AML/CFT-related information. Article 3(3) of the Law on Financial Market Supervision also specifically authorizes the NBS, where relevant, to share information about the shortcomings identified during the inspection of FIs with relevant foreign authorities.

Criterion 40.15 **–** Foreign supervisory authorities are allowed to carry out on-site inspections of branches and subsidiaries of their supervised FIs (third country supervisors need an agreement with the NBS), and to apply the same powers as the NBS including by conducting relevant inquiries under Article 4(1) of the Law on Financial Market Supervision. However, the authorities did not provide information as to whether the NBS is able to conduct inquiries on behalf of foreign counterparts.

Criterion 40.16 **–** Article 3(5) of the Law on Financial Market Supervision states that the NBS may use the information obtained from foreign counterparts for supervisory purposes, or when challenged in the court or required so as part of criminal prosecution. In all other instances that information can be provided to other authorities or persons only with the consent of the requested foreign supervisor.

Criterion 40.17 **–** The Police Force co-operates with the police of other states, with international police organisations, international organisations and organisations operating on the territories of other states, primarily by exchanging information, exchanging liaison officers, and other possible forms. The international cooperation of ARO and the exchange of information between national AROs is based on the procedures and deadlines set out in the EU Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of EU Member States No 2006/960/JHA. ARO/CARIN is an executive operational unit carrying out tasks resulting from Council Decision No 2007/845/JHA following the application of procedures and deadlines under Council Framework Decision No 2006/960/JHA, which defines rules for the execution and provision of background and information for the needs of members of an

international network of agencies involved in the cross-border identification, freezing, seizing and confiscation of proceeds of crime and other property related to crime. (Art. 77 (a) of the Law on PF). There are no references made to the capacity of other LEA for the purposes of identification and tracing of proceeds of crime. The AT was not provided with info on Customs ability to exchange information on ML and TF issues with foreign counter-parts.

Criterion 40.18 – According the Art 69da of the Act on the Police Forces, the Police can request and provide the information with all EU member states for the criminal proceeding purposes. In case of non-EU countries, Art. 69da(9) provides for the possibility to exchange information internationally provided that the third-party country has adequate guarantees regarding information protection. Internal legislation requires Police to cooperate with the National Central Bureaus providing international police cooperation – SIRENE, Interpol, Europol.

Criterion 40.19 – Art. 10 (9) CCP provides that The Joint Investigation Team (JIT) is a concept that can be used in the area of anti-money laundering by the Financial Police Unit NAKA as well as the Anti-Corruption NAKA under the applicable legislation. According to Art. 13 the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the EU, in 2014 – 2018 financial administration investigators were involved in five Joint Investigation Teams.

Criterion 40.20 – The CTU-NAKA accepts "indirect" requests as part of the international information exchange. The requests are handled within the scope of CTU-NAKA powers, if this is not possible, the request is sent to the competent authority. Under the AML/CFT Act, the FIU can exchange information with its domestic and foreign partners on the prevention, detection and prosecution of money laundering and terrorist financing on request or spontaneously. Information may also be exchanged with partners who are not FIUs, indirectly, upon request, either by domestic entities or foreign entities. The principles as stated in the paragraphs above apply to all such exchanged information (e.g., a police unit may demand information from the FIU for its partner unit abroad or, the FIU may demand information from a foreign FIU for a Slovak police unit, as well as provide a foreign FIU with information for the purpose of moving it to a foreign police unit). The provision of information also requires the consent of the FIU or the foreign FIU.

According to Article 18 (3)(a) of the Instruction of the National Criminal Agency of the Presidium of the Police Force on the organisational rules of the National Criminal Agency of the Presidium of the Police Force, CTU-NAKA in particular coordinates the fight against extremism and fight against terrorism within the Ministry of Interior of the Slovak Republic and Police Force, cooperating with respective bodies, organisations and institutions at a level of the Ministry and out of it, and at an international level.

Weighting and Conclusion

Slovakia meets most of the criteria under Recommendation 40. However, there are number of deficiencies in relation to the rules for the prioritisation and timely execution of the requests and legal provisions regarding the signature of the agreements. Also, some information was missed in relation to the information exchange and the possibility to conduct inquiries on behalf of foreign counterparts. Slovakia also meets minor limitations in the process of the FIU's information exchange. **R.40 is rated LC**.

Summary of Technical Compliance – Key Deficiencies

Recommendation	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	**PC**	• There are no timelines for the NRA up-dates in the AML/CFT Act. • There is no legal obligation to provide information about the results of the NRA. • Absence of the information on the RBA in allocation of resources and implementing measures to prevent and mitigate ML/TF. • There are no provisions to oblige the REs to take enhanced measures to manage and mitigate risks where higher risks are identified.
2. National cooperation and coordination	**LC**	• The Slovak Republic has an outdated version of the National Action Plan to Combat Terrorism.
3. Money laundering offence	**LC**	• There are discrepancies in the approach to the issue of the purposive element and coverage between the Conventions and the CC of the Slovak Republic. • Deficiencies in in the criminalization of the TF. • Absence of the criminalisation of the conspiracy to commit a basic money laundering offence. • There are some limitations to the criminalization of self-laundering.
4. Confiscation and provisional measures	**LC**	• There is no authority to take steps to prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation. • The rights of bona fide third persons are not clearly protected by substantive legislation. • The legislation does not expressly cover the confiscation of laundered property. • The third-party confiscation regime does not cover instrumentalities. • Management of seized and confiscated assets does not seem to extend beyond safekeeping measures.
5. Terrorist financing offence	**LC**	• Requirement to prove an intention 'to damage the constitutional establishment or defensibility of a

Recommendation	Rating	Factor(s) underlying the rating
		country…' is not in conformity with the FATF standard.
6. Targeted financial sanctions related to terrorism & FT	**LC**	• The Slovak Republic has no formalised procedure at the national level under which Slovakia could ask another country to give effect to freezing measures. • The are no clear designation criteria as set out in the relevant UNSCR. • Some Acts does not include the provision for the protection of bona fide third parties. •
7. Targeted financial sanctions related to proliferation	**LC**	• There is a certain lack of clarity in the establishment of the functions of the various state bodies in the PF TFS field. • Absence of the guidance for the implementing entities which are not financial entities. • Absence of the direct reference in the legislation to the obligation to "monitor" the compliance of FIs and DNFBPs. • The legislation has no clear reference to the list of guarantees as set out in the FATF Methodology
8. Non-profit organisations	**PC**	• The authorities have not identified the features and types of NPOs which are likely to be at risk of terrorist financing abuse. • There is no specific requirement to periodically re-assess the NPO sector. • Absence of the review of the adequacy of measures including the subset of NPO sector that may be abused for terrorism financing support. • There is no specific outreach to the NPO sector or the donor community on FT issues. • Absence of the developed practices in cooperation with NPOs regarding protection from the FT abuse.
9. Financial institution secrecy laws	**LC**	• There is a lack of specific exemptions from confidentiality provisions in relation to R.13, R.16 and R.17 which affect the overall rating.
10. Customer due diligence	**PC**	• Absence of full range of CDD measures when carrying out occasional wire transfers over EUR 1,000. • No legal requirement to verify whether persons act on behalf of third person are authorized and verify the identity of that person and the customer. • There is no requirement to verify BOs based on reliable source data. • No clear information provided regarding FI's understanding the purpose and intended nature of

Recommendation	Rating	Factor(s) underlying the rating
		the business relationship. • Absence of the specific requirement to examine, where necessary, whether transactions of the customer are consistent with the source of funds. • There is no obligation to understand the customer's business. • Number of the deficiencies regarding he identification and verification measures for legal persons and legal arrangements. • There are no specific requirements regarding beneficiaries designated by characteristics or class. • Absence of the similar definition of BOs for other types of legal arrangements. • Number of deficiencies regarding the CDD for beneficiaries of life insurance policies. • Absence of legal provisions that would require FIs to apply CDD to existing customers depending on the materiality. • Simplified CDD measures in low risk scenarios which are not justified by the findings of the NRA. • Absence of the requirement to refuse establishing a business relationship or performing a transaction, and to terminate a business relationship where FIs cannot perform other required CDD measures such as conducting ongoing due diligence. • Obligation to report unusual transactions does not broadly extent to the situation when a financial institution is unable to comply with the relevant CDD measures. • The legislation does not contain the permission for the FIs refrain from pursuing the CDD process in case of risk of tipping-off the customer followed by submission of a UTR.
11. Record keeping	**LC**	• There is no specific requirement to keep the records obtained through CDD measures for 5 years in regard to the occasional customers. • Business correspondence, account files, and the results of analyses undertaken outside the context of identifying unusual transactions are not covered by

Recommendation	Rating	Factor(s) underlying the rating
		the record-keeping requirements.
12. Politically exposed persons	**PC**	• There is no specific requirement to put in place risk management systems for identifying PEPs. • There is no specific requirement to take reasonable measures to establish the origin of the entire body of wealth of PEPs. • The definition of family members however does not include siblings of PEPs, which is part of the minimum standard provided by the FATF Guidance. • There is no requirement for the FIs providing life insurance policies to take reasonable measures to determine whether the beneficiaries or the BO are PEPs.
13. Correspondent banking	**PC**	• The correspondent banking requirements apply only to EU/EEA countries. • There is no requirement to determine if the respondent has been subject to a ML/FT investigation or regulatory action. • FIs are not specifically required to assess the quality of respondent FIs' AML/CFT controls. • FI's do not clearly understand the respective AML/CFT responsibilities of each institution.
14. Money or value transfer services	**LC**	• Absence of the information on the modalities of identifying the provision of unauthorized payment services by persons other than authorized institutions or the applicable criminal sanctions.
15. New technologies	**LC**	• There is no explicit requirement for risk assessment and mitigation to take place before launch of a new technology, product or service.
16. Wire transfers	**LC**	• There is no explicit obligation requiring payment service providers to file a UTR in any country affected by the suspicious wire transfer and to make relevant transaction information available to the FIU.
17. Reliance on third parties	**LC**	• FIs are not specifically required to satisfy themselves that third parties have measures in place to comply with the relevant CDD and record-keeping requirements. • FIs' prohibition to rely on third parties from countries placed on the EU list of high-risk jurisdictions is not equivalent to the obligation to have regard to information on the level of country risk.
18. Internal controls and foreign branches and subsidiaries	**PC**	• Absence of the obligation for the FIs to take into account the size of the business when designing AML/CFT programs. • Legal provision requiring FIs to screen their

Recommendation	Rating	Factor(s) underlying the rating
		employees to ensure high standards when hiring does not exist. • There is no specific requirement to put in place an independent audit function for the purpose of testing the AML/CFT system. • The requirement to implement group-wide AML/CFT programs does not extend to branches and subsidiaries in EU member states, as well as for the collection of the relevant customer, account and transaction data at the group-level functions, or the dissemination of those data to members of the group for risk management purposes. • Limited requirement to include adequate safeguards on confidentiality and prevention of tipping-off in the group-wide AML/CFT programs. • Requirements to the FIs' branches and majority-owned subsidiaries in third countries to take AML/CFT measures in line with the domestic and EU legislation do not extend to those who are placed in the EU member states.
19. Higher-risk countries	**PC**	• Enhanced CDD measures can only be applied to high-risk countries that are not part of the EEA area. • Lack of clarity whether enhanced CDD measures must be applied to natural persons who reside or legal persons that primarily operate in the high-risk jurisdiction. • The Slovak Republic is not able to apply countermeasures either independently or when called for by the FATF. • FIU is only publishing the decisions taken by the European Commission that identify high-risk jurisdictions with strategic deficiencies.
20. Reporting of suspicious transaction	**PC**	• The definition of the UTR is not in line with the FATF requirements. • The definition of the UTR has a strict referral to a link to ML rather than "proceeds of criminal activity". • The legislation requires that the legal act "can be used" for ML purposes rather than having suspicious or reasonable grounds to suspect.

Recommendation	Rating	Factor(s) underlying the rating
		• The legislation refers to the possibility for the operations to "be used" for TF rather than being "related" to TF.
21. Tipping-off and confidentiality	**LC**	• The exemptions do not cover all civil and criminal liability for breaches of confidentiality clauses. • No clarity if the exemption applies in cases where FIs and their employees did not know precisely what the underling criminal activity was and whether illegal activity occurred.
22. DNFBPs: Customer due diligence	**LC**	• Shortcomings identified under Recs. 10, 11, 12, 15 and 17 equally apply to DNFBPs. • TCSPs are not required to apply CDD measures when performing the equivalent function of a trustee for another form of legal arrangement.
23. DNFBPs: Other measures	**PC**	• Shortcomings identified under Recs. 18, 19 and 21 equally apply to DNFBPs. • TCSPs are not required to report suspicious transactions when performing the equivalent function of a trustee for other forms of legal arrangement
24. Transparency and beneficial ownership of legal persons	**LC**	• Insufficiently comprehensive assessment of ML/TF risks associated with all types of legal persons created in the country. • The legal framework does not cover sanctioning for false submissions. • Absence of requirement to retain the information after the company is dissolved or otherwise ceases to exist. • Limited number of the legislative provisions requiring companies and registers to check the accuracy of the beneficial ownership information. • Absence of the formal processes to monitor the quality of assistance from abroad
25. Transparency and beneficial ownership of legal arrangements	**LC**	• Shortcomings identified under Rec. 10 regarding BOs and their verification equally apply to this Recommendation. • Absence of the legislation that governs trusts or other types of legal arrangements. • The requirement to establish the identity of the BO do not obliging trustees to disclose their status to FIs and DNFBPs. • Absence of the registration of the TCSPs what can become a legal obstacle in getting access the BO data recorded in a timely manner. • Limited direct obligations for trustees affect legal liability of trustees and sanctions.

Recommendation	Rating	Factor(s) underlying the rating
26.Regulation and supervision of financial institutions	**PC**	• Insufficient steps to guard the insurance sector against the associates of criminals • Absence of the information on measures to prevent criminals or their associates from holding or being the BO of the significant interest in an insurance undertaking. • Frequency and intensity of onsite or of-site AML/CFT supervision of financial institutions/group are based on an investigation plan not on the ML/TF risks. • There is no actually risk classification or risk mapping of the FIs supervised. • The risk classifications/profile do not affect the intensity or scope of supervision applied to individual insurance undertakings.
27.Powers of supervisors	**LC**	• Absence of the information regarding the legal processes for withdrawing, restricting or suspending the license of other FIs' for AML/CFT violations
28.Regulation and supervision of DNFBPs	**PC**	• Absence of the measures in place to prevent associates of criminals from holding management functions in DNFBPs. • Frequency and intensity of supervision is not based on a risk-sensitive basis. • The sanctions for violations of AML/CFT requirements concern only the entities and do not apply to persons performing management functions in DNFBPs. • There are no checks applied in relation to holders or BOs of significant or controlling interest in DNFBPs.
29.Financial intelligence units	**PC**	• The legislation does not clearly determine the "regulation" setting up the FIU. • The FIU's position and its core-functions definitions are volatile due to repeated changes within the Police structure and the reference made to the FIU in various pieces of legislation is done in an inconsistent manner. • There is no clear legal obligation for the FIU to carry out strategic analyses. • the Head of the FIU is not able to conclude MOUs

Recommendation	Rating	Factor(s) underlying the rating
		independently • Wide ranging of the dissemination of the information creates deficiencies in its protection. • There is no legal provision on how the FIU files are archived.
30. Responsibilities of law enforcement and investigative authorities	**PC**	• No LEAs clearly designated to investigate ML offences with special responsibility. • No LEA specifically designated to carry out identification, search and seizure of suspected criminal proceeds or property subject to confiscation. •
31. Powers of law enforcement and investigative authorities	**LC**	• Interception and recording of telecommunications are not applicable to all potential predicate offences. • Absence of the possibility of the direct access to the computer systems. • In lack of a central register of bank accounts, the existing mechanism of written requests for banking information does not ensure a timely performance.
32. Cash couriers	**PC**	• Absence of the EU-internal border declaration system for cash or BNIs. • Absence of co-ordination among customs, immigration and other related authorities on issues relevant for R32. • The legislation does not provide power to stop or restrain cash/BNIs for a reasonable period of time to check the existence of the evidence of ML/FT. • Sanctions for non-declaration or false declarations are not dissuasive enough. • The completed declaration forms are submitted to the FIU only on a monthly basis. • Transportation of cash/BNIs by legal persons and/or cross-border transportation of cash/BNIs via mail and cargo are not covered by the legislation.
33. Statistics	**PC**	• There are no statistics on the ML and TF investigations; • The statistics kept on seizures are incomplete (do not distinguish between proceeds, instrumentalities or property of equivalent value; • There are no statistics on confiscations and assets recovered.
34. Guidance and feedback	**LC**	• Not all important aspects of the AML/CFT regime are covered by the published Guidelines. • The provisions of the AML/CFT Act regarding

Recommendation	Rating	Factor(s) underlying the rating
		feedback are of a general nature.
35. Sanctions	**PC**	• Sanctions cannot be applied to natural persons such as senior management of obliged entities. • Absence of proportionate and dissuasive sanctions or violations of terrorism & terrorism financing related TFS.
36. International instruments	**LC**	• Shortcomings identified under Recs. 3 and 5 equally apply to this Recommendation.
37. Mutual legal assistance	**C**	
38. Mutual legal assistance: freezing and confiscation	**PC**	• The mechanism for enforcing non-EU confiscation orders does not allow for an expeditious action. • Shortcomings identified under Rec. 4 regarding mechanisms for managing, and when necessary disposing of, property frozen, seized or confiscated. • Absence of explicit legislative regulation for sharing of confiscated assets with non-EU countries.
39. Extradition	**LC**	• Absence of clear processes for timely execution of extradition requests other than EAWs.
40. Other forms of international cooperation	**LC**	• Absence of the mechanism for the prioritisation and timely execution of the requests. • Absence of the legal provisions regarding signature of the agreements. • No information provided from the NBS and the Police regarding the possibility to conduct inquiries on behalf of foreign counterparts • Absence of the information on Custom's ability to exchange information on ML and TF issues with foreign counterparts. • There are limitations regarding the FIU's exchange with non-EU FIUs.

Glossary of Acronyms[69]

ARO-NAKA	Property Investigation Department
BO	Beneficial Owner
CARIN	Camden Assets Recovery Inter-Agency Network
CFT	Combating the financing of terrorism
CTU-NAKA	Counter-Terrorism Unit NAKA
DB	Database
DMS	Document Management System
EAW	European Arrest Warrant
EC	European Commission
EIO	European Investigation Order
EJN	European Judicial Network
ESW	Egmont Secure Web
EU	European Union
EVO	Vehicle records
FACO	Criminal Office for Financial Administration
FDSR	Financial Directorate of Slovakia
FI	Financial Institution
Fintech	Financial Technology
FIU	Financial Intelligence Unit
FT	Financing of terrorism
GDP	Gross Domestic Product
GPO	General Prosecutor's Office
GRA	Gambling Regulatory Authority
IBE	Institute of Banking Education
IMF	International Monetary Fund
INTERPOL	International Police Organisation
ISA	International Sanctions Act
KAPOR	Real property register
LEA	Law Enforcement Agency
MEKO	Interdepartmental Expert Coordination Body on Combating Crime
MER	Mutual Evaluation Report
ML	Money Laundering
MLA	Mutual Legal Assistance
NAKA	National Criminal Agency Slovakia
NAP	National Action Plan
NBS	National Bank of Slovakia
NES-FT	National Expert Group on Counter-Terrorist Financing (Sub-Group of NES-LP)
NES-LP	National Expert Group on Anti-Money Laundering
NPKJ	National Anti-Corruption Unit
NRA	National Risk Assessment
NSAC	National Security Analytical Center
OC	Organized crime
OCG	Organised Crime Group
ORSR	Commercial Register
RBA	Risk Based Approach
REs	Reporting entities
RTVS	Public Broadcaster of Slovak Republic
SIS	Slovak Information Service
MI	Military Intelligence
SPO	Special Prosecutor Office of the General Prosecutor's Office
TF	Terrorism financing
TI	Transparency International
UMPS	Office of International Police cooperation of the Police Force Presidium
USP	Special Prosecutor's Office

69 Acronyms already defined in the FATF 40 Recommendations are not included into this Glossary.

UTR	Unusual transaction report
WMDs	Weapons of mass destruction

www.coe.int/MONEYVAL

September 2020

Anti-money laundering and counter-terrorism financing measures

Slovak Republic

Fifth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in the Slovak Republic as at the date of the on-site visit (6 to 18 October 2019). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of the Slovak Republic's AML/CFT system, and provides recommendations on how the system could be strengthened.