

Slovak Republic

Fifth Round Mutual Evaluation Report 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. 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 Effectiveness and Technical Compliance

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 Risks, coordination and policy setting (Chapter 2 - IO.1; R.1, R.2, R.33 & R.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, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.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 Financing and Financing Proliferation (Chapter 4 - IOs 9-11; R.5-8)

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.

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 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 - IO4; 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 - IO3; R.26-28, R. 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 of Legal Persons and Arrangements (Chapter 7 - IO5; 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 - IO2; 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 Ratings¹

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
ME	SE	ME	ME	ME	ME
IO.7 - ML & investigation prosecution	IO.8 - Confiscation	IO.9 - FT & investigation prosecution	IO.10 - FT preventive measures & financial sanctions	IO.11 - PF financial sanctions	
ME	LE	ME	ME	ME	

Technical Compliance Ratings (C – compliant, LC – largely compliant, PC – partially compliant, NC – non compliant, N/A – not applicable)²

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		

¹ Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness.

² Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non compliant.

All rights reserved. Reproduction is authorised, provided the source is acknowledged, save where otherwise stated. For any use for commercial purposes, no part of this publication may be translated, reproduced or transmitted, in any form or by any means, electronic (CD-Rom, Internet, etc.) or mechanical, including photocopying, recording or any information storage or retrieval system without prior permission in writing from the MONEYVAL Secretariat, Directorate General of Human Rights and Rule of Law, Council of Europe (F-67075 Strasbourg or moneyval@coe.int).

© MONEYVAL

www.coe.int/MONEYVAL