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

MONEYVAL(2011)21

Report on Fourth Assessment Visit

Anti-Money Laundering and Combating the Financing of Terrorism

SLOVAK REPUBLIC

26 September 2011

The Slovak Republic is a member of MONEYVAL. This evaluation was conducted by MONEYVAL and the report on the 4th Assessment Visit was adopted by MONEYVAL at its 36th Plenary (Strasbourg, 26 - 30 September 2011).

TABLE OF CONTENTS

LIST OF ACRONYMS USED

AML/CFT	Anti-Money Laundering and Counter-Terrorist Financing
AML/CFT Act	Act No. 297/2008 Coll. on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing (hereinafter referred to as AML/CFT Act)
ATM	Automatic Telling Machine
CARIN	Camden Asset Recovery Interagency Network
SCC	Criminal Code
CDD	Customer Due Diligence
CSD	Central Securities Depository
CIS	Collective Investments Act
CPC	Criminal Procedure Code
DNFBP	Designated Non-Financial Businesses and Professions
EAW	European Arrest Warrant
ECDD	Enhanced Customer Due Diligence
ESW	Egmont Secure Web
EU	European Union
FIU	Financial Intelligence Unit ("Spravodajská Jednotka Finančnej Polície" in Slovakia)
FMS Act	Act No. 747/2004 Coll. On Supervision of the Financial Market
IIEG	Interagency Integrated Group of Experts
IT	Information Technology
MEQ	Mutual Evaluation Questionnaire
MER	Mutual Evaluation Report
MLA	Mutual Legal Assistance
MoF	Ministry of Finance
MOU	Memorandum of Understanding
NBS	National Bank of Slovakia
NPO	Non-Profit Organisation
ML	Money Laundering
PEPs	Politically Exposed Persons
SCC	Slovak Criminal Code
SCDD	Simplified Customer Due Diligence
SROs	Self-Regulatory Authorities
STR	Suspicious Transaction Report
TF	Terrorist Financing
UN	United Nations
UNSCR	United Nations Security Council Resolution
UTR	Unusual Transaction Report

I. PREFACE

1. This is the fifth report in MONEYVAL's 4th round of mutual evaluations, following up the recommendations made in the 3rd round. This evaluation follows the current version of the 2004 AML/CFT Methodology, but does not necessarily cover all the 40+9 FATF Recommendations and Special Recommendations. MONEYVAL concluded that the 4th round should be shorter and more focused and primarily follow up the major recommendations made in the 3rd round. The evaluation team, in line with procedural decisions taken by MONEYVAL, have examined the current effectiveness of implementation of all key and core and some other important FATF recommendations (i.e. Recommendations 1, 3, 4, 5, 10, 13, 17, 23, 26, 29, 30, 31, 35, 36 and 40, and SR I, SR II, SR III, SR IV and SR V), whatever the rating achieved in the 3rd round.

2. Additionally, the examiners have reassessed the compliance with and effectiveness of implementation of all those other FATF recommendations where the rating was Non-Compliant (NC) or Partially Compliant (PC) in the 3rd round. Furthermore, the report also covers in a separate annex issues related to the Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter the "The Third EU Directive") and Directive 2006/70/EC (the "Implementing Directive"). **No ratings have been assigned to the assessment of these issues.**

3. The evaluation was based on the laws, regulations and other materials supplied by Slovakia, and information obtained by the evaluation team during its on-site visit to Slovakia from 4 to 9 October 2010, and subsequently. During the on-site visit, the evaluation team met with officials and representatives of relevant government agencies and the private sector in Slovakia. A list of the bodies met is set out in Annex I to the mutual evaluation report.

4. The evaluation was conducted by an assessment team, which consisted of members of the MONEYVAL Secretariat and MONEYVAL and FATF experts in criminal law, law enforcement and regulatory issues and comprised: Mr Professor William C. Gilmore (Professor of International Criminal Law at the University of Edinburg and Scientific expert to MONEYVAL) and Mr Paul Landes (Head of the Israel's FIU) who participated as legal evaluators, Mr. Radoslaw OBCZYNSKI (Specialist, AML/CFT Unit - Enforcement Department - Polish Financial Supervision Authority) and Ms Marta Fernandez MARTIN (Advisor, AML/CFT Unit - Spanish Treasure General Directorate) who participated as financial evaluators, Mr Milovan MILAVANOVIC (Head of International Department in the Serbian FIU) who participated as a law enforcement evaluator and Mr John RINGGUTH and Mr Sener DALYAN, members of the MONEYVAL Secretariat. The experts reviewed the institutional framework, the relevant AML/CFT laws, regulations, guidelines and other requirements, and the regulatory and other systems in place to deter money laundering (ML) and the financing of terrorism (FT) through financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs), as well as examining the capacity, the implementation and the effectiveness of all these systems.

5. The structure of this report broadly follows the structure of MONEYVAL and FATF reports in the 3rd round, and is split into the following sections:

    1. General Information
    2. Legal System and Related Institutional Measures
    3. Preventive Measures - Financial Institutions
    4. Preventive Measures – Designated Non-Financial Businesses and Professions

5. Legal Persons and Arrangements and Non-Profit Organisations
6. National and International Cooperation
7. Statistics and Resources

Annex (implementation of EU standards).
Appendices (relevant new laws and regulations)

6. This Report on the 4th Assessment Visit should be read in conjunction with the 3rd round adopted mutual evaluation report (as adopted at MONEYVAL's 20th Plenary meeting from 12 to 15 September 2006), which is published on MONEYVAL's website[1]. The FATF Recommendations that have been considered in this report have been assigned a rating. For those ratings that have not been considered the rating from the 3rd round MER continues to apply.

7. Where there have been no material changes from the position as described in the 3rd round MER, the text of the 3rd round MER remains appropriate and information provided in that assessment has not been repeated in this report. This applies firstly to general and background information. It also applies in respect of the 'description and analysis' section discussing individual FATF Recommendations that are being reassessed in this report and the effectiveness of implementation. Again, only new developments and significant changes are covered by this report. The 'recommendations and comments' in respect of individual Recommendations that have been re-assessed in this report are entirely new and reflect the position of the evaluators on the effectiveness of implementation of the particular Recommendation currently, taking into account all relevant information in respect of the essential and additional criteria which was available to this team of examiners.

8. The ratings that have been reassessed in this report reflect the position as at the on-site visit in 2010 or shortly thereafter.

[1] http://www.coe.int/moneyval

II. EXECUTIVE SUMMARY

Background Information

1. This report summarises the major anti-money laundering and counter-terrorist financing measures (AML/CFT) that were in place in Slovakia at the time of the 4th on-site visit (4 to 9 October 2010) and immediately thereafter. It describes and analyses these measures and offers recommendations on how to strengthen certain aspects of the system. The MONEYVAL 4th cycle of assessments is a follow-up round, in which Core and Key (and some other important) FATF Recommendations have been re-assessed, as well as all those for which Slovakia received non-compliant (NC) or partially compliant (PC) ratings in its 3rd round MER. This report is not, therefore, a full assessment against the FATF 40 Recommendations and 9 Special Recommendations but is intended to update readers on major issues in the Slovak AML/CFT system.

Key Findings

2. Slovakia enacted on 1 September 2008 a new Act No. 297/2008 Coll. on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing transposing the Third EU Money Laundering Directive, and Implementing Directive. Overall, the new law has brought the Slovak preventive AML/CFT system broadly into line with the FATF standards. Notably it established a clear legal basis for reporting suspicions of financing of terrorism, which was missing at the time of the last evaluation.

3. Even though no formal action plan (at policy level) aiming at reviewing the implementation of AML/CFT policies domestically was adopted by the Government after the adoption of the 3rd round mutual evaluation report (MER) for the implementation of the recommendations, most of the elements of the action plan as set out in the 3rd round MER appear to have been addressed and significant progress has continued to be made since the adoption of the 3rd round MER in September 2006.

4. The evaluators were not advised of any specific AML/CFT risk assessment undertaken since the last evaluation. Nonetheless, they were advised that there is a significant threat from domestic organised crime investing its proceeds overwhelmingly within the Slovak economy. Other prevalent economic and financial crimes include official corruption, theft of vehicles, tax evasion, fraud, and smuggling.

5. The authorities consider the TF risk to be low. The major improvement with regard to the fight against terrorist financing since the adoption of the 3rd round MER has been the incrimination of financing of terrorism offence as an autonomous offence which is broadly in line with the international standards, though some issues, as noted beneath, remain outstanding.

6. Overall, Slovakia has continued to develop and strengthen its AML/CFT regime since the adoption of the 3rd round MER. There is, however, still a very low level of prosecutions for money laundering (ML) (and, though this is less clear, of orders to confiscate assets). The evaluators have serious concerns about how effectively money laundering is being used as a tool to fight major proceeds-generating crime and organised crime. Given the centrality of the FIU in the Slovak AML/CFT system, its present level of resources and position in the overall police structure, as well as its operational independence and autonomy, still needs to be further strengthened.

Legal Systems and Related Institutional Measures

7. Several modifications have been introduced to the Slovak Criminal Code (SCC) resulting in the present legislation, which has brought ML incrimination largely in compliance with the Vienna and Palermo Conventions. However, some uncertainties and shortcomings still appear to remain. The "property" for the purposes of the money laundering offence has not yet been clearly defined in the criminal legislation, which was also raised as a deficiency in the 3rd round MER. The requirement of the purposive element of "concealing the origin of the thing" for the laundering acts under Section 233 appears to impose an extra burden on the practitioners for the acts of disguising of or possession or use of the property for personal use.

8. The 3rd round MER noted the lack of criminal, civil or administrative sanctions for ML offences applicable to legal persons as deficiencies. Slovakia, with the enactment of the Act no. 224/2010 Coll. amending the Criminal Code, has introduced what may be regarded as a form of criminal liability for legal persons. These amendments came into force on 1 September 2010 and make it possible to impose protective/security measures on legal entities and confiscation of a property belonging to a legal entity. The sanctions applicable for natural and legal persons for ML offences appear to be effective, proportionate and dissuasive.

9. The statistics provided do not show how many convictions relate to third party laundering on behalf of others, as opposed to self-laundering, or indeed, how many cases were generated by the police through financial investigations in parallel with their investigations into the predicate offences. The available ML statistics present a low number of convictions and agreements on guilt and punishment. Furthermore, the use of ML offence in the context of use of stolen cars, which in many jurisdictions would generally be prosecuted as receiving offences, continues to be a feature of criminal prosecution in this area. Car theft is the predicate offence in no less than 62% of the money laundering cases, since in total 292 out of 471 cases were linked to car theft. Furthermore, theft of other things or documents consists of 37 cases in total, which increases the offences treated as receiving offences to 70% of the money laundering cases. The evaluators consider that prosecution of crimes of these types as ML offences is not the primary goal of the AML regime. There is no evidence of money laundering prosecutions or convictions in relation to major and more serious proceeds-generating cases perpetrated by organised crime or others for pure economic gain. Therefore, the reasons for the discrepancy between the extent of organised crime in Slovakia and the type and quality of ML cases brought forward (and which have resulted in convictions) need to be analysed by the Slovak authorities.

10. The evaluation team welcomed the amendments made to the Slovak Criminal Code that came into force on 1 January 2010, which introduced an autonomous TF offence into Slovak law as recommended as a matter of urgency in the 3rd round MER. However, a number of shortcomings still prevent it from being fully in line with the requirements of Special Recommendation II. The financing of an individual terrorist's day-to-day activities is not criminalised as required under SR II. In addition, the Slovak Criminal Code needs to be revised so as to fully incriminate the financing of some of the acts defined in the treaties listed in the annex to the UN Terrorist Financing Convention. As there had been no investigations, prosecutions and convictions for TF offences in Slovakia at the time of the on-site visit, the existing legislative framework has not been tested in practice.

11. The legislative steps taken by Slovakia since the adoption of the 3rd round MER has brought the Slovak general criminal freezing and confiscation system more into line with the international standards, though further steps are needed for full compliance. The Slovak Republic however could not demonstrate that the implementation of freezing and confiscation measures is being effectively pursued, as no meaningful statistical information on freezing and confiscation were made available.

12. The implementation of SR.III relies primarily upon the application of binding EU legislation. However, to supplement current EU procedures, a requirement to freeze assets of EU-internals was adopted by the Government Regulation No. 397/2005 Coll. (on execution of international sanctions to ensure international peace and security). Certain generic shortcomings which exist in the EU Regulation apply also in Slovakia. The Slovak Government Regulation contains the list of sanctioned persons, whose activity is confined to the territory of EU Member States or EU nationals. Financial institutions in Slovakia are obliged to freeze immediately all funds and economic assets of the persons included on the list in the Annex to Government Regulation No. 397/2005 Coll. Nevertheless, Slovakia does not have any effective national law or procedure, apart from the EU's mechanism, to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions, which ensure the prompt determination and the subsequent freezing of funds or other assets without delay. Slovakia does not have a publicly available procedure in place for any individual or entity to apply for a review of the designation from the designating authority, with the ability to seek further review of an adverse finding by the designating authority, to a review body. Similarly, there is no specific procedure which deals with unfreezing in a timely manner the funds or other assets of persons or entities inadvertently affected by a freezing mechanism, upon verification that the person or entity is not a designated person. As at the time of the 3rd round mutual evaluation still there are no appropriate measures in place for monitoring the effective compliance with SR III. As no guidance was provided to DNFBPs and financial institutions other than banks, and the level of awareness of these sectors in respect of the freezing obligations still needs increasing. There has been no case of freezing of assets under the UNSCRs, which raises the concerns about the effectiveness of the existing procedures.

13. The AML/CFT Act defines the FIU as the national unit for the area of prevention and detection of money laundering and terrorist financing. The Act describes in detail the competences of the FIU. The FIU, one of departments of the Bureau for Combating Organised Crime of the Presidium of Police Force, is central to the Slovak AML/CFT system. The 3rd round MER emphasised its rather weak position in the overall police structure. Other than defining its roles and competencies more clearly in the new AML/CFT Act, no substantive steps have been taken by the authorities to strengthen the position of the FIU in the system. That said, it should be noted that the evaluators have not found any indication that the operational independence of the FIU has been affected so far by this issue. Nevertheless, reiterating the findings of the previous report, the present evaluators identified a continued lack of legal safeguards to ensure the FIU's operational independence and autonomy. Employees in the FIU have direct access to a variety of police databases and publicly available sources, which were integrated within a satisfactory IT system. This enables it to act quickly and effectively in its analytical functions.

14. The FIU is required to disseminate cases to law enforcement bodies which relate to all criminal offences, not just ML and TF. Especially, internet fraud activities like phishing and pharming have a significant place in the FIU's daily work. Moreover, the FIU is obliged to inform tax authorities of possible tax evasion cases, and to maintain a separate database of information extracted from unusual transaction reports, which information is made available to the security service in Slovakia. The Slovak authorities consider that, as a police unit, the FIU should not concentrate on just a few specific criminal offences. They noted that the FIU analyses and disseminates information on all criminal offences equally, which they consider adds value to the FIU's work. The evaluators none-the-less consider that these additional requirements do not allow the FIU to concentrate sufficiently on ML and TF. This gives rise to concerns about the effectiveness of the overall AML/CFT system in place, bearing in mind that the AML/CFT Act itself puts the FIU at the centre of that system, with responsibility for co-ordination and development of the whole system. The FIU employees are professional and motivated. The FIU shows a very high level of dedication to its responsibilities. It is however debatable whether their large responsibilities can be performed with the present level of resources and its current position in the overall police structure.

15. The present cross-border declaration system in Slovakia is based on the directly applicable EU Regulation; hence it only applies to the movements at the borders between Slovakia and non-EU Member States. In addition to the EU Regulation, there are several other laws in place which are used in Slovakia in order to implement requirements of SR IX. A very low number of declared transfers of cash or other bearer negotiable gives rise to concerns about the effectiveness of the implementation of the declaration system. Moreover, no cases of false declarations or failure to declare have been recorded.

Preventive Measures – Financial Institutions

16. As an EU Member State Slovakia was required to implement the Third EU AML/CFT Directive (Directive 2005/60/EC) and the implementing Directive 2006/70/EC). The Act No. 297/2008 Coll. of 2 July 2008 on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing and on Amendments and Supplements to Certain Acts as amended by the acts No. 445/2008 and No. 186/2009 entered into force on the 1st September 2008. The Act implements the Third EU AML/CFT Directive in Slovakia, and stipulates basic rights and obligations of legal entities and natural persons in the prevention and detection of legalisation of proceeds of criminal activities and terrorist financing. Overall, the new AML/CFT Act has addressed most of the deficiencies identified in the 3rd round MER and established the legal preventive AML/CFT framework broadly in line with the FATF standards.

17. Slovakia has adopted and implemented a risk-based approach to AML/CFT, particularly in relation to customer/beneficial owner identification and verification requirements. Pursuant to the AML/CFT Act financial institutions are entitled to specify the extent of customer due diligence measures on a risk-sensitive basis and apply it to all their customers.

18. Implementation of CDD requirements by banks has been recorded as quite effective, since they have developed a comprehensive preventive regime. Though most of the other financial sector representatives met on-site seemed to have a good understanding of international AML standards, some of them, such as securities pension funds and payment services, appeared to be less aware of the ML risks and threats in their sectors. A need for issuing methodological guidelines for each sector, as has been provided for the banking sector, in order to improve general performance of CDD measures, is noted in the report. The new AML/CFT Act has introduced the concept of PEPs into the Slovak law, though the definition of PEPs should be revisited to ensure the full coverage of the definition provided in the Glossary to the FATF Recommendations in terms of senor politicians, senior government officials and important party officials.

19. The legislation on financial institution secrecy appears to enable the authorities to access the information that they require in order to exercise their functions in the fight against money laundering and terrorist financing, and does not inhibit the implementation of the FATF Recommendations. Furthermore, no problems appear to have been experienced in practice.

20. Overall, the record-keeping requirements, which are embedded in Section 19 of the AML/CFT Act and in the sectoral laws, are broadly in line with the FATF standards. Nevertheless, there is still no legal obligation that requires the maintenance of account files and business correspondence.

21. One of the important deficiencies in the 3rd round evaluation was the absence of any broad requirement for financial institutions to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations. This situation still remains unchanged. The Slovak law still does not have a requirement for financial institutions to pay special attention to such relationships and transactions. Similarly, the Slovak authorities are not in a position to apply countermeasures at present as required under Recommendation 21.

22. Significant improvements have been made in the reporting system since the 3rd round evaluation. The obligation to report unusual transactions is stipulated in Section 17 of the AML/CFT Act. Unusual transaction is defined in the Act as a legal act or other act which indicates that its execution may enable legalisation or terrorist financing. The AML/CFT Act goes further in defining unusual transaction, implicitly providing reporting entities with some guidance or indicators for recognising suspicion. The Act requires obliged entities to postpone an unusual transaction if there is a danger that its execution may hamper or substantially impede seizure of proceeds of criminal activity or funds intended to finance terrorism. With the adoption of the new AML/CFT Act a clear legal basis for reporting suspicions of financing of terrorism now exists and attempted transactions are now clearly covered within the scope of the reporting obligation. Deficiencies in the definition of terrorist financing in the AML/CFT Act could have a negative impact on the reporting of TF related suspicious transactions. The reporting level from the banking and, to some extent, insurance sector appears to be satisfactory. However, other financial institutions show a significantly lower level of reporting. This gives rise to concerns about the effectiveness of the reporting regime. There are not indicators for recognising suspicious transactions as guidelines for other financial sectors (securities market, currency exchange etc).

23. The requirements of the AML/CFT Act relating to the obligations to create an internal control system, internal procedures, policies to prevent ML and TF are broadly in line with the FATF standards.

24. There have been important changes in the supervisory structure for financial institutions in Slovakia since the adoption of the 3rd round MER. For instance, the NBS has been the single supervisory authority over the entire financial market in the Slovak Republic since January 2006. The procedure which is being used by the NBS during on-site visits is comprehensive; however, more training for the NBS staff focusing on TF is needed. Gambling operators and internet casinos are supervised by the Ministry of Finance. Supervision of the financial sector over AML/CFT issues is conducted by the FIU. The NBS and the Ministry of Finance, before starting an on-site visit, inform the FIU of the business name, place of business or registered office, identification number and type of obliged entity which is to be controlled. After a control is completed the FIU is made aware of the results and measures taken. If the NBS or the Ministry of Finance detects an unusual transaction or other facts that may be associated with ML or TF, the FIU is informed without undue delay. The authorities are also authorised to conduct on-sites together. Even though no sole body responsible for sanctioning has been explicitly named, there have been no cases of double sanctioning and the co-operation between the NBS and the FIU seems to be on a good level. Further improvement is needed in co-operation between the FIU and the Ministry of Finance. The evaluators believe that overall the supervisory system works properly. The range of sanctions that may be imposed by the supervisory authorities is wide and the sanctions are effective, proportionate and dissuasive. However, some sanctions stipulated in the sectoral laws cannot be imposed by the FIU as it is not authorised to impose sanctions on directors and senior management of financial institutions.

Preventive Measures – Designated Non Financial Businesses and Professions (DNFBP)

25. Overall the meetings with the DNFBP sector demonstrated that, apart from the external auditors, the DNFBP sector in general is not aware at all of their obligations arising from the AML/CFT Act. Although some outreach activities have been performed by the FIU, the provision of more extensive outreach to this sector on their obligations is urgently needed. The low number of STRs, in the opinion of the evaluators, is evidence of inadequate implementation of the FATF standards. This was also a deficiency identified in the 3rd round evaluation. Only 1 UTR has been received from lawyers (in 2006) and 8 from notaries since the adoption of 3rd round MER. Only 2 UTRs have been reported by real estate agencies and a very low number of STRs has been reported by accountants and auditors. No data has been made available as to whether dealers in precious metals and stones have ever reported any UTRs. Leaving aside some legislative refinements, the same

concerns identified in the 3rd round MER over the effectiveness of the implementation in all aspects of these Recommendations, remain valid.

26. All of the DNFBPs mentioned in Section 5 of the AML/CFT Act are under the supervision of the FIU apart from the gambling sector, which is supervised also by the Ministry of Finance. Some of them (lawyers, auditors, accountants and tax advisers) have their own SROs. This does not limit the powers of the FIU for AML/CFT related supervision. Given the statistics on on-site visits and the size of the unit (the FIU), as well as the number of entities to be supervised, the evaluators consider that supervision over this sector cannot be conducted effectively by the FIU with its present level of resources.

Legal Persons and Arrangements & Non-Profit Organisations

27. No comprehensive review appears to have been made of commercial, corporate, and other laws with a view to taking measures to provide adequate transparency with respect to the beneficial ownership, as recommended in the 3rd round MER. Therefore, the deficiencies regarding this Recommendation still appear to remain valid. This evaluation team reiterates the findings of the 3rd round evaluators that Slovak law still does not require adequate transparency concerning beneficial ownership and control of legal persons. It appears that, since the adoption of the 3rd round MER, insufficient steps have been taken to bring the Slovak system into conformity with SR.VIII. A review of the sector has still not been undertaken and there has been insufficient outreach to the NPO sector. Concerns remain about the transparency of the sector and insufficient steps have been taken to strengthen the legal basis for supervision and oversight over NPO fundraising.

National and International Co-operation

28. The authorities have a variety of mechanisms in place to facilitate co-operation and policy development. There are also mechanisms to facilitate co-operation between the agencies involved in investigating ML and TF. More effective mechanisms however are needed at operational level. The authorities need to consider the creation of joint investigative teams or other forms of operational interagency co-ordination mechanisms in order to investigate and bring before the courts more money laundering cases which are related to major proceed-generating criminal offences.

29. Slovakia has ratified the Vienna and Palermo Conventions and the UN Terrorist Financing Convention. The legislation has been amended in order to implement the Conventions, but existing legislation does not cover the full scope of these Conventions. Furthermore, measures still need to be taken in order to properly implement UNSCRs 1267 and 1373.

30. Legal provisions for providing mutual legal assistance are laid down in domestic law, bilateral and multilateral treaties and apply both to ML and FT and the possible forms of international co-operation cover a wide range of forms.

31. The Slovak authorities appear to have sufficient powers to enable them to provide different forms of assistance, information and co-operation without undue delay or hindrance. The responses received to MONEYVAL's standard enquiry on International Cooperation which was sent to MONEYVAL and FATF members were generally positive. However, deficiencies identified in relation to the definition of the TF offence might limit the ability of Slovak authorities to provide mutual legal assistance in TF cases.

Other Issues

32. While internal co-operation between the FIU and the NBS appears to be satisfactory, especially in the area of outreach and providing guidance to entities in the financial sector, more emphasis needs

to be placed on enhancing the quality and frequency of day-to-day co-operation involving other stakeholders. Deficiencies in this co-operation have the potential to hamper the effectiveness of the Slovak AML/CFT regime.

33. Notwithstanding the existence of the Integrated Interagency Group of Experts, at a more strategic level, it appears to the evaluators to be essential that steps be taken to ensure that the national AML/CFT risk and the overall effectiveness of the national AML/CFT system are assessed on a regular basis.

III. MUTUAL EVALUATION REPORT

1 GENERAL

1.1 General Information on Slovakia

1. As noted in the 3rd round MER, Slovakia acceded to the European Union in 2004. Slovakia is bordered by Austria, the Czech Republic, Hungary and Poland within the EU, and has one external EU border, with Ukraine. Its population is approximately 5,429,763 (as at June 2010). The official currency of Slovakia has been the Euro since the 1st January 2009.

2. The reader is referred to the 3rd round Mutual Evaluation Report for the details of the form of government and principles of its legal system.

Economy

3. During the years 2006 to 2010, Slovakia has witnessed both economic growth and a short recession. During the period 2006 to 2008, there was strong economic growth, accompanied by falling unemployment and growing activity in corporate sector. This growth was supported by solid lending activity in both the corporate and household sectors. The global financial crisis hit Slovakia at the end of 2008. Falling business activity was very soon followed by growing unemployment, which together led to an increase in non-performing loans. The year 2009 was characterised by a high uncertainty, a decrease in real estate prices, and a further decrease in business activity and a significant slowdown in banks' lending. The situation improved in 2010, when growing exports and industrial production contributed to GDP growth. Also, lower uncertainty in the labour market contributed to strong growth of housing loans. Although most of the signals are positive, uncertainty about activity in some business sectors remains relatively high.

Table 1: Economic indicators

	2006	2007	2008	2009	2010
GDP €bn. (current prices)	55.08	61.56	67.01	63.05	65.91
GDP €bn. (constant prices 00)	42.98	47.50	50.27	47.86	49.79
GDP year growth in % (current prices)	11.70	11.76	8.85	-5.91	4.54
(constant prices)	8.51	10.52	5.83	-4.79	4.03
GDP per capita €'ooo's (current prices)	10.22	11.41	12.39	11.64	12.14
(constant prices)	7.97	8.80	9.30	8.83	9.17
Inflation rate (HICP)	4.3%	1.9%	3.9%	0.9%	0.7%

Table 2: Overview of the Slovak financial sector in terms of total assets

	Assets (€m)		Structure (%)		% of GDP	
31 December	**2009**	**2010**	**2009**	**2010**	**2009**	**2010**
Monetary financial institutions						
Banks	53,028	54,695	71.77	70.95	84.10	82.98
Credit co-operatives	0	0	0.00	0.00	0.00	0.00
Non-monetary financial institutions						
Insurers	6,135	6,438	8.30	8.35	9.73	9.77
Pension companies/funds	3,947	4,863	5.34	6.31	6.26	7.38
Investment funds	4,121	4,497	5.58	5.83	6.54	6.82
Leasing Companies	3,375	3,091	4.57	4.01	5.35	4.69
Brokerage companies, management companies	1,946	2,199	2.63	2.85	3.09	3.34
Others (Factoring, Hire purchase companies)	1,338	1,302	1.81	1.69	2.12	1.98
Total	**73,889**	**77,085**	**100.00**	**100.00**	**117.19**	**116.96**

1.2 General Situation of Money Laundering and Financing of Terrorism

Recorded Criminal Offences

4. Slovakia's geographic, economic, and legal environment with respect to money laundering are not atypical of a changing central European economy. Its geographical location makes it a transit country for trafficking in drugs, people, and a variety of commodities. Money laundering in Slovakia is related to a variety of criminal activities, including illicit narcotics-trafficking and organised crime. Other prevalent economic and financial crimes include official corruption, theft of vehicles, tax evasion, fraud, and smuggling. The authorities reported on-site that about 95% of illicit proceeds in Slovakia resulted from economic crimes (such as bribery in public tenders in tenders, tax and customs fraud, smuggling and fictitious export of goods from Slovakia to abroad) and illicit drug related offences. The evaluators were advised on-site that there is a significant threat from domestic organised crime investing its proceeds overwhelmingly within the Slovak economy especially in real estate. The evaluators were further informed that not only criminals hide the proceeds of crimes themselves but also there are some organised groups that are active in this field some of which try to establish clearing societies or companies before investigations in their activities.

5. The information reported to the evaluators on money laundering cases investigated and prosecuted by Slovak authorities since 2005 revealed the most frequent predicate offence for money laundering is motor vehicle theft, as it was in the 3rd round evaluation. The main categories of offence that the Slovak Financial Intelligence Unit (hereinafter referred to as FIU) identified and disseminated as a result of notifications received were money laundering suspicions related to tax offences, fraud, establishing, contriving and supporting a criminal group, sharing, unlawful manufacturing and use of electronic payment means and other payment card and trafficking in migrants.

6. The Slovak authorities provided the evaluators with the number of reported offences causing damage and estimated amounts of economic loss resulting from major proceeds generating offences. The evaluators were also provided with the number of investigations and convictions on FATF designated categories of offences as shown in the tables below:

Table 3: The Number of Recorded Criminal Offences[2]

	2005	2006	2007	2008	2009	2010
CRIMINAL OFFENCES AGAINST PROPERTY						
Theft	37.833	37.936	37.102	33.743	31.549	14.630
Burglary	20.828	19.044	17.148	15.159	15.394	7.575
Fraud	5.259	3.576	3.762	3.795	3.867	2.140
Robbery	1.576	1.594	1.429	1.371	1.358	636
Theft of vehicles	5.591	5.225	4.719	4.135	3.779	1.709
Concealment	29	24	21	21	25	15
Other CO against property	6.645	6.097	5.795	5.853	5.456	2.410
CRIMINAL OFFENCES OF ECONOMIC NATURE						
Business fraud	---------	----------	-------	-------	--------	--------
Fraud	4.246	6.540	4.048	3.302	3.369	1.279
Issuing of an uncovered cheque, misuse of a credit card	1.287	1.870	2.342	2.507	2.625	1.020
Tax evasion		287	872	1.226	2.320	961
Forgery	55	692	829	594	320	138
Abuse of authority or rights	64	29	200	184	202	113
Embezzlement	2.976	685	1.197	1.349	1.475	794
Usury	7	15	17	26	26	19
Abuse of insider information	9	19	4	9	3	2
Abuse of financial instruments market		3	2	2	------	-------
Unauthorised use of another's mark or model		75	378	225	104	69
Other CO of economic nature	10.601	8.952	8.006	7.550	9.074	4.640
OTHER CRIMINAL OFFENCES						
Production and trafficking with drugs	830	1.678	2.111	2.256	2.432	915
Illegal migration	93	130	170	33	43	18
Production and trafficking with arms	546	539	458	505	526	255
Falsification of money		586	666	662	2.062	944
Corruption	97	166	211	178	160	89
Extortion	1.230	891	874	868	719	390
Smuggling	107	22	31	8	19	28
Murder, grievous bodily harm	4.002	3.295	3.056	2.798	2.706	1.418
Prohibited crossing of state border or territory, trafficking in human beings	17	33	33	36	32	12
Violation of material copyright		46	107	92	44	30
Kidnapping, false imprisonment		116	134	113	130	62
Burdening and destruction of environment	192	153	137	119	233	109
Unlawful acquisition or use of radioactive or other dangerous substances		13	1	1		2
Pollution of drinking water				1	1	
Tainting of foodstuffs or fodder	2		2			
TOTAL	**98.531**	**95.106**	**91.143**	**85.586**	**86.274**	**40.713**
Other Criminal Offences (Not Included Above) against life and limb, human rights, honour, sexual integrity, public health, etc.	**25.032**	**20.045**	**19.659**	**19.173**	**18.631**	**9.873**
NUMBER OF ALL CRIMINAL OFFENCES	**123.563**	**115.151**	**110.802**	**104.759**	**104.905**	**50.586**

[2] Annual police reports for 2005, 2006, 2007, 2008, 2009 and first half of 2010

Table 4: The number of investigations and convictions for FATF Designated Categories Offences

FATF designated categories of offences	2006		2007		2008		2009		First half of 2010	
	Investigations	Convictions	Investigations	Convictions	Investigations	Convictions	Investigations	Convictions	Investigations	Convictions
Participation in organised criminal group and racketeering										
▪ §186,189,190, 191, 192	257	301	614	319	666	353	649	352	613	160
Terrorism and terrorist financing										
▪ § 419	0	0	0	0	0	0	0	0	0	0
▪ § 297	0	0	0	1	0	0	0	0	0	0
Trafficking in human beings and migrant smuggling										
▪ § 179, 180, 181, 355	33	50	145	128	115	114	59	69	94	30
Sexual exploitation and sexual exploitation of children										
▪ § 199-202	199	200	460	244	480	232	433	264	383	126
Illicit trafficking in narcotic drugs and psychotropic substances										
▪ § 171- 174	622	722	1583	786	1842	911	2202	1079	2143	577
Illicit arms trafficking										
▪ § 294, 295	79	104	287	160	270	185	319	218	298	94
Illicit trafficking in stolen and other goods										
▪ § 252-257	20	46	24	11	20	11	21	4	12	0
Corruption and bribery										
▪ § 328-336,	3	84	14	122	14	97	5	124	185	69
Fraud										
▪ § 221-226, 213	826	3564	3291	3392	5114	4120	5275	4182	5382	2147
Counterfeiting currency										
▪ § 219, 270, 271	163	143	402	159	501	204	679	267	557	167
Counterfeiting and piracy of products										
▪ § 275	5	4	19	10	9	2	5	0	7	0
Environmental crimes										
▪ § 300-310	334	196	458	184	476	168	624	259	578	102
Murder, grievous bodily injury										
▪ § 144-163	1651	2443	4595	2726	3963	3022	4999	2906	4328	1439
Kidnapping, illegal restraint and hostage-taking										
▪ § 209, 210, 182-185, 187	58	75	147	61	143	62	57	59	160	35
Robbery or theft										
▪ § 212, 215-218, 188	7927	6277	12633	6840	13384	7164	15017	8270	14641	4542
Smuggling										
▪ § 254-256	9	4	19	5	14	8	8	3	6	2
Extortion										
▪ § 189	251	294	582	305	635	337	623	345	582	153
Forgery										
▪ § 220, 270-275	54	104	146	81	136	86	134	79	115	37
Piracy										
▪ § 281-283	17	33	123	70	166	100	103	57	113	34
Insider trading and market manipulation										
▪ § 265-269, 269a	0	11	0	11	12	2	5	3	16	1

Suspicious transaction reports from reporting entities

7. With respect to the reporting of suspicious transactions, the situation has changed since the last evaluation. Overall, the number of STRs has steadily increased, with a slight decline in 2010. In 2006, there were 1,471 STRs and in 2007 there were 1,920 STRs. The overall number of STRs has increased from 2,173 in 2005 to 2,741 in 2009. A slight decline was recorded in 2010 as 2,470. While 10,846 STRs were received for the period from 2006 to 2010, only 151 STRs (14 in 2006; 10 in 2007; 16 in 2008; 56 in 2009 and 55 in 2010) were related to terrorist financing, the remaining STRs were related to money laundering cases. Banks have been reporting the highest number of STRs. Out of the total of 10,997 STRs; banks reported 9,443 STRs (85% of the total number of STRs 1 January 2006 and 31 December 2009).

Cases disseminated to the competent authorities

8. Slovak authorities could provide the evaluators with the statistics on the disseminations of the STRs only for 2009 and 2010 in the period from 1 January 2009 to 31 December 2010; the FIU forwarded 1,677 case reports to law enforcement authorities and 961 reports to tax authorities. 111 of those case reports notified to law enforcement authorities were related to terrorist financing. While the number of indictments based on the notifications was 68 in 2009, it dramatically declined to 4 in 2010.

The most common methods of money laundering identified in notifications sent to law enforcement authorities

9. The most common methods of ML identified in notifications sent to law enforcement authorities by the FIU are:

    1. chains of business companies declaring system of payments,
    2. the use of off-shore companies and companies residing abroad,
    3. the use of safe deposit boxes,
    4. money mules, couriers, front person,
    5. electronic transfer of money via Western Union,
    6. investments in real estate,
    7. placement of illegal income into the legal system – mixing illegal proceeds with legal proceeds,
    8. the use of proceeds of criminal activity for legal business – establishment of business company and loans.

ML investigations, prosecutions and convictions

10. As will be seen below, the statistics provided (See statistics under Recommendation 1 and 2) by the authorities give limited information to the evaluators. The statistics related to ML indicate only the number persons investigated, prosecuted and convicted, whilst the number of investigations, prosecutions and convictions could not be made available to the evaluators. According to the data provided, the number of persons convicted for ML (Section 233 of the SCC) was 12 in 2007; 10 in 2008; 8 in 2009 and 13 in 2010. Authorities provided the information as to the number of investigations conducted by the prosecution service; however, as noted below, due to the inconsistencies between the different sets of statistics, it has not been possible for the evaluators to infer reliable conclusions from those statistics.

Property frozen, seized and confiscated

Table 5: Estimated Economic Loss of the Recorded Criminal Offences[3](in thousands of Euro)

	2005	2006	2007	2008	2009	2010
CRIMINAL OFFENCES AGAINST PROPERTY						
Theft	106.236	103.661	97.085	88.974	81.922	32.891
Burglary	36.559	34.771	36.935	34.783	34.048	17.055
Fraud	251.851	110.067	112.514	86.867	97.731	90.922
Robbery	5.545	1.828	3.137	2.822	1.606	797
Theft of vehicles	65.119	62.298	58.433	51.092	51.193	20.186
Concealment	0	0	0	0	0	0
Other CO against property	5.668	6.766	6.275	6.471	6.942	3.505
CRIMINAL OFFENCES of ECONOMIC NATURE						
Business fraud	---------	----------	-------	-------	--------	--------
Fraud	46.572	25.972	32.545	20.110	14.013	5.549
Issuing of an uncovered cheque, misuse of a credit card	1.040	1.244	1.527	2.290	3.310	653
Tax evasion	-	14.686	37.304	52.798	140.340	79.072
Forgery	0	270	41	121	33	408
Abuse of authority or rights	2.940	6.058	488	559	1.176	10.622
Embezzlement	524.145	7.388	23.321	26.894	28.804	10.903
Usury	0	65	114	55	30	40
Abuse of insider information	100	116	1.362	15	3.056	0
Abuse of financial instruments market	-	-	-	-	-	-
Unauthorised use of another's mark or model		0	7.638	229	165	865
Other CO of economic nature						
OTHER CRIMINAL OFFENCES						
Production and trafficking with drugs	0	0	0	0	0	0
Illegal migration	0	0	0	0	0	0
Production and trafficking with arms	33	114	35	36	115	3
Falsification of money		129	30	80	62	40
Corruption	0	0,1	0	0,03	0	0
Extortion	2.245	473	953	661	531	1.486
Smuggling	1.130	402	2.730	154	3.908	517
Murder, grievous bodily harm	25	29	36	89	9	5
Prohibited crossing of state border or territory, trafficking in human beings	0	0	0	0	0	0
Violation of material copyright	-	26	4.232	101	20	510

[3] Annual police reports for 2005, 2006, 2007, 2008, 2009 and first half of 2010.

Kidnapping, false imprisonment	-	1,1	17	1,4	0	0
Burdening and destruction of environment	4.127	1.771	3.556	3.004	1.037	1.615
Unlawful acquisition or use of radioactive or other dangerous substances						
Pollution of drinking water	0	-	0	60	0	0
Tainting of foodstuffs or fodder						
Approximate economic loss or damage of all criminal offences	**1.935.567**	**474.239**	**557.840**	**454.197**	**496.373**	**319.593**

Terrorist financing in Slovakia

11. Regarding terrorist financing, the situation has not changed over the last few years. The Slovak authorities still estimates its general vulnerability to the international terrorism to be low in comparison to that of other countries in the European Union. As is shown below, the major improvement with regard to the fight against terrorist financing since the adoption of the 3rd round has been incrimination of financing of terrorism offence as an autonomous offence which is being broadly in line with the international standards.

1.3 Overview of the Financial Sector and Designated Non-Financial Businesses and Professions (DNFBPs)

Financial Sector

Banking sector

12. As of 31 December 2009 (according to the National Bank of Slovakia Annual Report 2009) the Slovak financial system was composed of 15 banks and 16 branches of foreign banks (2 of which did not commence banking activity). There were also 2 branches of a Slovak bank operating abroad. Furthermore, there were 271 banks and 13 e-money institutions which are entitled to freely provide cross-border banking services in Slovakia.

13. At the time of the adoption of the 3rd round mutual evaluation report (MER), the banking sector remained the most important component of the financial sector. It now amounts to 70.95 % of financial market assets (as at the end of 2010).

14. The procedure for granting licences to e-money institutions to perform these activities is regulated by the Act No. 492/2009 Coll. on Payment Services (hereinafter referred to as "Payment Services Act"). Such institutions can be established in the legal form of a joint stock company or a legal entity established as Business Company that is obliged to create registered capital (paragraph 2 of Article 82 of the Payment Services Act).

Foreign exchange business providers

15. Since the 1st January 2009 the Slovak Republic has introduced Euro as its currency. The evaluators were advised by the NBS and the service providers that the introduction of Euro has resulted in a significant decrease in the number of foreign exchange business providers, as the role of this sector has significantly dropped since then.

16. The NBS keeps and publishes a full and updated list of foreign exchange offices on its website. The number of foreign exchange offices, as at the end of September 2010, was 1,187 and that of non-cash foreign exchange currencies exchange providers was 9. On the other hand, the number of foreign exchange cash cross-border transfer providers was 1.

17. The National Bank of Slovakia issued 17 licences for currency exchange activities in 2009.

Securities Market

18. The Slovak capital market may be described as rather small in comparison with other stock exchange centres in the region. Nonetheless, there are 8 domestic asset management companies and 78 domestic mutual funds in the Slovak financial market.

19. As at 31 December 2009, there were 18 Investment firms as defined by the Securities Act. 14 of them were banks. By the same time, there were 125 securities issuers whose securities are admitted as being traded on a regulated market. In addition, there were 962 investment service intermediaries, of which 877 were natural persons and 85 legal persons.

20. There were also 6 pension fund management companies. Apart from investment service intermediaries, all the above-mentioned financial institutions are joint stock companies.

Insurance Sector

21. As at 31 December 2009, there were 20 registered insurance companies in the Slovak insurance market. These comprised:
    - 12 composite insurance companies (offering both life and non-life insurance);
    - 5 life insurance companies; and
    - 3 non-life insurance companies.

22. There were also 447 insurance companies from other EU Member States operating in the Slovak insurance market, of which 433 operated on a freedom to provide services basis (without establishing a branch) and 14 through branches. However, as of December 2009, there was no reinsurance company operating in Slovakia.

Designated Non-Financial Businesses and Professions (DNFBPs)

23. There are no significant changes to this particular sector in respect of the catalogue of the major DNFBP since the 3rd round evaluation. It should, however, be noted that at the date of the on-site visit there were 3 casinos operating companies in Slovakia.

1.4 Overview of Commercial Laws and Mechanisms Governing Legal Persons and Arrangements

24. By the Act no. 24/2007 Coll. which amended the Act no. 530/2003 Coll. on Commercial Register, the possibility of electronic request for incorporation was introduced. Apart from this amendment, there have been no major changes in the commercial laws and mechanisms governing legal persons and arrangements since the 3rd round evaluation. Therefore, the information given in the 1.4 of the 3rd round MER is apt and the reader is referred to that report for the details.

1.5 Overview of Strategy to Prevent Money Laundering and Terrorist Financing

a. AML/CFT Strategies and Priorities

25. The 3rd round MER described and analysed the AML/CFT measures in place in Slovakia as at mid-2005, and provided recommendations on how certain aspects of the system could be strengthened. After its adoption at the 20th MONEYVAL plenary meeting (12 to 15 September 2006), the report was presented to the Government of Slovakia. Apart from establishment of the Integrated Group of Experts (hereinafter referred to as IIEG), no formal action plan (at policy level) aiming at reviewing the implementation of AML/CFT policies domestically was adopted by the Government after the adoption of the 3rd round MER for the implementation of the recommendations.

26. However, most of the elements of the action plan as set out in the 3rd round MER appear to have been addressed and significant progress has continued to be made since the adoption of 3rd round MER.

27. The IIEG, which is headed by the Head of the FIU, was established in 2008. The IIEG meets regularly with the participation of representatives or relevant domestic authorities and submits its conclusions to the Deputy Prime Minister and the Minister of Interior. Its task is to deal with the issues related to the AML/CFT at the national level especially by taking measures fully compliance with the EU standards. It currently works with a working plan with identified areas, which should be addressed and these are as follows:
    - Application of the new AML/CFT Act in practice;
    - To secure fully compliance of the preventive measures adopted by the Slovak Republic with the EU Law;
    - To set up a central registry of bank accounts;
    - To ensure the maintaining of detailed statistics for all respective bodies – Ministry of Justice, General Prosecutor's Office and to provide these figures to the FIU which will publish a summary review of that statistical data in an annual report;
    - To analyse the provisions of the Criminal Code on money laundering and taking appropriate measures *(e.g. a problem identified: an over emphasis on criminal evidence in respect of predicate offence with no money laundering and assets seizure orientation)*;
    - To ensure rigorous implementation of the Order of the President of the Police Forces No. 5/2009 which obliges investigators to prove all the criminal proceeds, their placing, nature, status and price within criminal proceedings as well as to detect and investigate money laundering offence.
    - To amend the Criminal Procedure Code in order to ensure seizing of money on a bank account completely including "facility" (for example incoming money to the account).

28. After the 3rd round MER, the overall policy objectives were to further improve the Slovak legal and institutional AML/CFT framework. Upon the adoption of the third AML/CFT Directive by the EU, Slovakia considered the preparation of a new AML/CFT law so as both to harmonise its legislation with the 3rd EU Directive and to improve its existing AML/CFT legal framework.

29. Slovakia has implemented the 3rd AML/CFT Directive by the Act No. 297/2008 Coll. on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing (hereinafter referred to as AML/CFT Act) which entered into force on 1 September 2008. The text of the law is set out in Annex III.

b. The approach concerning risk

30. Details of the current Slovak approach concerning risk are set out in section 3.1.

c. Progress since the last mutual evaluation

Developments in the legal framework

31. The main AML/CFT legislative enhancement has been the preparation, adoption and implementation of a new AML/CFT Law that came into force on 1 September 2008. The new Law was intended to implement the "Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing" (hereinafter referred to as 3rd EU AML/CFT Directive)), and the "Commission Directive 2006/70/EC of 1 August 2006 which provides implementing measures for Directive 2005/60/EC of the European Parliament and of the Council particularly in respect of the definition of "politically exposed person" and the technical criteria for simplified customer due diligence procedure and for exemptions on the grounds of financial activity conducted on an occasional or very limited basis" (hereinafter referred to as the Implementation Directive) and replaced the previous AML/CFT Law.

32. The new preventive law introduced some major changes concerning requirements on obliged entities as discussed in this Report. Overall, the new law has brought the Slovak preventive AML/CFT system broadly in line with FATF standards. Notably it establishes a clear legal basis for reporting suspicions of financing of terrorism, which was missing at the time of last evaluation.

33. Furthermore, as described below in the sections on Recommendation 1 and Special Recommendation II in more depth, a new Criminal Code (Act No. 300/2005 Coll.) (Hereinafter referred to as SCC) and Criminal Procedure Code (Act No. 301/2005 Coll.) (Hereinafter referred to as CPC) were brought into force on 1 January 2006, which made some important improvements (including to the ML offence). Since then, the SCC has been amended several times to further improve AML/CFT provisions. Whilst the amendments made to the SCC on the 1st January 2010 introduced an autonomous TF offence, the latest amendment of the SCC (Act No. 224/2010 Coll.) established corporate liability in the Slovak legal system for listed offences including ML, TF terrorism and corruption. The latter came into force shortly before the on-site visit on the 1st September 2010.

34. Following the Constitutional Court judgment a new Act No. 291/2009 Coll. on Specialised Criminal Court was adopted and brought into force on 17 July 2009. By this Act the former Special Court was dissolved and the new Specialised Criminal Court was created. This new court continues the work of the Special Court. However, some concerns of the Constitutional Court in its decision of 20 May 2009 were remedied. The Act no. 291/2009 Coll. amended some relevant provisions of the Criminal Procedure Code, Act on Courts and other relevant legal regulations. As to the powers of the Specialised Criminal Court, according to the Section 14 of the Criminal Procedure Code amended by the Act no. 291/2009 Coll., the Specialised Criminal Court shall have the jurisdiction over the persons in respect of:
    a) criminal offence of first degree murder,
    b) criminal offence of deceitful practices in public procurement and public auction pursuant to Section 266 paragraph 3 of the Criminal Code,
    c) criminal offence of forgery, fraudulent alteration and illicit manufacturing of money and securities pursuant to Section 270 paragraph 4 of the Criminal Code,
    d) criminal offence of abuse of power by a public official pursuant to Section 326 paragraph 3 and 4 of the Criminal Code in concurrence with criminal offence pursuant to letters b), c), e), f), g), j) or k),
    e) criminal offences of passive bribery pursuant to Section 328 through 331 of the Criminal Code,
    f) criminal offences of active bribery pursuant to Section 332 through 335 of the Criminal Code,

g) criminal offence of trading in influence pursuant to Section 336 of the Criminal Code,
h) the criminal offence of establishing, masterminding and supporting a criminal group and the criminal offence of establishing, masterminding and supporting a terrorist group,
i) particularly serious crimes committed by a criminal group or a terrorist group,
j) criminal offences against property under Chapter Four of the Special Part of the Criminal Code or economic criminal offences under Chapter Five of the Special Part of the Criminal Code, if such criminal offence causes a damage or brings a benefit which is at least twenty-five thousand times higher than the amount of small damage set out in the Criminal Code, or if the extent of that offence is at least twenty-five thousand times higher than the amount of small damage set out in the Criminal Code,
k) criminal offences against financial interests of the European Communities,
l) criminal offences related to those referred to under a) to j) or k), provided that the requirements for the joinder of proceedings are met.

35. Slovakia signed the Convention of the Council of Europe No. 198 on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (hereinafter referred to as Convention No. 198) on 12 November 2007 and ratified it on 16 September 2008. The Convention No. 198 came into force in Slovakia on the 1st January 2009.

36. The National Council (Parliament) of the Slovak Republic adopted the UN Convention against Corruption, signed on 9 December 2003, by its Resolution no. 2145 dated on 15 March 2006 and then the President ratified it on 25 April 2006. It came into force in Slovakia as of the 1st July 2006.

37. The Methodological Guideline of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing to enhance a proper AML/CFT Law application in the practice was issued by the Financial Market Supervision Unit of the National Bank of Slovakia in co-operation with the FIU and the Ministry of Finance. Through non-binding and thus non-enforceable tool, numerous clarifications and recommendations to the newly established, more detailed obligations in line with the 3rd EU AML/CFT Directive and the Implementation Directive, and also supervisory expectations towards market players have been presented by it.

Institutional Developments

38. Since January 2006, the National Bank of Slovakia (hereinafter referred to as NBS), has been the single supervisory authority over the financial market in the Slovakia. The general procedural rules followed by the NBS in supervising and regulating the financial market in the areas of banking, capital market, insurance and pension savings are laid down in Act No. 747/2004 Coll. on Supervision of the Financial Market and on amendments to certain laws as amended (hereinafter referred to as FMS Act), which entered into force on the 1st January 2006. The supervisory and regulatory powers defined in this law are exercised by the Financial Market Supervision Unit, which was until the end of June 2010 managed by a Vice-Governor of the NBS. The organisation of this Unit has been changed by the Bank Board of NBS since 1 July 2010. The unit is currently under the direct authority of an executive director with 3 departments:
    - supervision over banking sector & payment services providers (including FX offices),
    - supervision over the securities, insurance and pension markets,
    - regulation and financial analysis (including banking & payment services regulation section, which among other responsibilities encompasses also the prevention of ML/TF in financial market).

39. A new analytical department within the FIU, composed of 6 people including IT specialists, was established on 1 April 2009.

2 LEGAL SYSTEM AND RELATED INSTITUTIONAL MEASURES

Laws and Regulations

2.1 Criminalisation of Money Laundering (R.1 and 2)

2.1.1 Description and analysis

Recommendation 1 (rated LC in the 3rd round MER)

Legal framework

40. Slovakia has signed and ratified the 1988 United Nations (UN) Convention on Illicit Drugs and Psychotropic Substances (Vienna Convention) and the 2000 UN Convention against Transnational Organised Crime (Palermo Convention). The offence of money laundering has been criminalised in the Slovak Criminal Code (hereinafter referred to as SCC). Since the 3rd round evaluation several modifications have been introduced resulting in the present legislation, that is now largely in compliance with international standards. On 1 January 2006, the new Criminal Code (Act no. 300/2005 Coll.) and Criminal Procedure Code (act no. 301/2005 Coll.) entered into force.

Criminalisation of money laundering (c.1.1 – Physical and material elements of the offence)

41. The money laundering offence was criminalised in Section 252 of the former SCC, but the evaluators of the 3rd round evaluation noted that the physical elements of the offence were not entirely consistent with the language of the Vienna and Palermo Conventions. The new SCC incriminates ML offences under Sections 231 (sharing), 232 (negligent ML) and 233 (legalisation of the proceeds of crime). However, from the texts of Sections 231 and 233 it is not easy to see at first glance how these different offences coexist in practice and how they are used by the courts. The offences under Sections 231 and 233 differ from one another in a few principle ways. Firstly, Section 231 refers only to sharing in the proceeds of another person's criminal offence, as is made clear by the wording used: "Any person who conceals …. a thing obtained through a criminal offence committed by another person, or." Section 233, on the other hand, refers to laundering the proceeds of a crime committed by any person. According to the Slovak authorities, self-laundering is thus punishable only pursuant to Section 233. In addition, Section 231 criminalises "sharing"- that is, using or consuming a thing with the aim of benefiting from it, while Section 233 criminalises "legalisation"- i.e. 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. Furthermore, Section 231 involves a thing gained by a criminal offence or a thing gained in exchange for such a thing, while Section 233 involves income or other property obtained by crime.

42. Section 231 of the SCC, entitled "Sharing", provides as follows:

"(1) Any person who conceals, transfers to himself or another, leases or accepts as a deposit

a) a thing obtained through a criminal offence committed by another person, or
b) anything procured in exchange for such a thing,
shall be liable to a term of imprisonment of up to three years.

(2) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to in paragraph 1,
a) and obtains larger benefit for himself or another through its commission,
b) by reason of specific motivation, or
c) uses such thing for his own business purposes.

(3) The offender shall be liable to a term of imprisonment of seven to twelve years if he commits the offence referred to in paragraph 1,
a) and obtains substantial benefit for himself or another through its commission, or
b) acting in a more serious manner.

(4) The offender shall be liable to a term of imprisonment of twelve to twenty years if he commits the offence referred to in paragraph 1,
a) and obtains large-scale benefit for himself or another through its commission, or
b) as a member of a dangerous grouping."

43. As seen from the text, the first paragraph of this Section criminalises the receiving offence. According to this Section, if a person conceals, transfers to himself or another person, leases or accepts as a deposit a thing obtained through a criminal offence committed by another person, the person shall be liable to a term of imprisonment of up to three years. On the other hand the remaining paragraphs of Section 231 incriminate the aggravated forms of this offence. Therefore, from the broad language used here, it can be concluded that this Section criminalises the acts of "concealment of the true nature, source, location, disposition, movement or ownership of or rights with respect to property", "transfer of property", "acquisition of property" and "use" of the property, but only "for his own business purposes". Since there is no other condition required by the Section, those acts are penalised irrespective of the purpose of the defendant.

44. Section 233 of the SCC, entitled "Legalisation of the Proceeds of Crime", reads as follows:

"1) Any person who performs any of the following with regard to income or other property obtained by crime with the intention 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:
transfers to himself or another, lends, borrows, transfers in a bank or a subsidiary of a foreign bank, imports, transits, delivers, transfers, leases or otherwise procures for himself or another, or holds, hides, conceals, uses, consumes, destroys, alters or damages,
shall be liable to a term of imprisonment of two to five years.

(2) The offender shall be liable to a term of imprisonment of three to eight years if he commits the offence referred to in paragraph 1
a) by reason of specific motivation, or
b) and obtains larger benefit for himself or another through its commission.

(3) The offender shall be liable to a term of imprisonment of seven to twelve years if he commits the offence referred to in paragraph 1
a) as a public figure,
b) and obtains substantial benefit for himself through its commission, or
c) acting in a more serious manner.

(4) The offender shall be liable to a term of imprisonment of twelve to twenty years if he commits the offence referred to in paragraph 1,
a) and obtains large-scale benefit for himself or another through its commission,
b) with respect to things originated from the trafficking in narcotics, psychotropic, nuclear or high risk chemical substances, weapons and human beings or from another particularly serious felony, or
c) as a member of a dangerous grouping."

45. In turn, Section 233 reproduces the main physical elements set out in the Vienna and Palermo Conventions. Although the physical and material elements of the money laundering offence criminalised under Section 233 do not strictly follow the definition of Vienna and Palermo Conventions, the broad language used in that section seems to comprise the elements listed in Article 3(1)(b) & (c) and Article 6(1) of these Conventions respectively. However, some uncertainties and shortcomings still appear to remain.

46. First of all, while Section 233 criminalises the conversion or transfer of property for the purpose of concealing or disguising the illicit origin of the property or frustrating their seizure for the purposes of criminal proceedings or forfeiture or confiscation, it does not incriminate 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 or her action as required by the Vienna and Palermo Conventions. However, the evaluators note that when a transfer for the purpose of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action occurs this act might be regarded as sharing offence under Section 231 as this section does not require any special purposive element for "transfer". In any case, conversion for the purpose of helping any person is covered neither in Section 231 nor in 233. Nevertheless, the evaluators accepted the claim of the Slovak authorities that Section 339 (See Annex V) of the SCC covers any action committed for the purpose of helping any person to evade the legal consequences of his or her actions, and therefore would also cover conversion or transfer of property for such purposes.

47. Secondly, Section 233 of the SCC requires that, to constitute a ML offence, existence of one of the purposive elements of concealing or disguising the illicit origin of the property or frustrating their seizure for the purposes of criminal proceedings or forfeiture or confiscation "purpose of concealing the origin of the thing" for the all laundering acts is required. Whereas Article 1(b) (i) of the Vienna Convention and Article 6 1(a) of the Palermo Convention allows and requires such a purpose element only for the acts of conversion and transfer of property. In turn purposive element is not required under Section 231 only for acts of concealing, transferring, leasing or accepting a thing as a deposit a thing or using it for his own business purposes. That is Section 233 appears to impose an extra burden on the practitioners for the acts of disguising of or possession or use of the property for personal use. Though this seems to be a theoretical discussion, the evaluators note that in these cases the penalty will be a term of imprisonment of up to three years and in the case of using for his own business purposes it will be a term of imprisonment of three to eight years, which are lower than the penalties that can be imposed under Section 233.

48. The Vienna and Palermo Conventions require the incrimination of laundering acts with special knowledge of the fact that such property is the proceeds of crime. Sections 231 and 233 do not make any reference to the knowledge of the defendant. However, the explicit non-referral to "knowledge" was not regarded as an obstacle to the "knowledge" element by the evaluators.

The laundered property (c.1.2) & Proving property is the proceeds of crime (c.1.2.1)

49. Section 233 of the SCC uses the words "income or other property" and Section 231 uses the word "thing". Section 130 of the SCC defines the word "thing" as including, *inter alia*, a movable or immovable thing, dwelling or non-residential premises, or animal (unless the relevant provisions of

the SCC provide otherwise), a controllable force of nature or energy, a security paper irrespective of its form. The definition of "thing" does not comply with the definition of "property" in the "Glossary of definitions used in the Methodology", which defines property as "assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets".

50. The evaluators were advised that the offence extends to any type of property on the basis of Slovak civil law. However, it was not clear if the definitions of the civil law apply to the SCC. Although the Slovak authorities provided a Supreme Court case relating to the definition of property for the purposes of the process of legal protection against offences against property, the evaluators were not convinced that this was sufficient to indicate a clear definition of the term "property" for the purposes of the money laundering offence or to fulfil the requirements of criterion 1.2. This was also raised as a deficiency in the 3rd round MER.

51. Regarding c.1.2.1, the Slovak prosecutorial authorities indicated there is no legal requirement that there be a prior conviction for a predicate offence in order to convict for money laundering. Despite the lack of information about autonomous convictions, based on the interviews held with various interlocutors the evaluators were willing to accept the prosecutors' position regarding the legal situation and to conclude that this criterion is met.

The scope of the predicate offence (c.1.3) & Threshold approach for predicate offences (c.1.4)

52. The ML offences in the SCC (Section 231 and 233) are based on the "all crimes approach" (a thing obtained through criminal offence (Section 231) - income or other property obtained by a crime (Section 233)). Under the Methodology, predicate offences have to cover at a minimum the range of offences in each of the designated categories of offence annexed to the FATF Recommendations. Section 233 refers to income obtained by a "crime", which is defined in Section 11 of the SCC as "an intentional criminal offence carrying a maximum custodial penalty of more than five years pursuant to the Special Part of this Act". Based on this definition, all of the categories of predicate offences are technically covered by the Criminal Code, since at least one offence within each category is subject to a punishment of more than five years imprisonment, under certain circumstances. Although some of the articles referred to by the Slovak authorities do not require punishment over five years or require such punishment only when certain more serious circumstances exist (see, for example, articles, 294, 231, 232, 254, 328, 332, 355 and others), the Slovak authorities referred the evaluators to Case No. 83/2005, which indicated that conviction for money laundering was possible even when the predicate offence was committed under circumstances that did not permit punishment exceeding five years. Therefore, this criterion appears to be met.

Extraterritorially committed predicate offences (c.1.5)

53. ML offences are punishable under Slovak law irrespective of the place where the predicate offence was committed. The SCC does not require that the latter offence be committed domestically, provided it would constitute a criminal offence/crime punishable under the SCC had it occurred domestically, that means by the term "property obtained by crime" (Section 233) or "obtained through a criminal offence"(Section 231) extraterritorial crimes are also covered to the extent that dual criminality exists. Section 232 of the SCC explicitly states that the criminal offence giving rise to the ML offence can be "committed in the territory of the Slovak Republic or abroad", while the other articles relating to these offences (231, 233) are silent regarding this point. Despite this fact, the evaluators accepted the Slovak authorities' claim that all these offences are fully applicable on all predicate offences regardless of where they are committed (so long as the act is punishable under the SCC if committed in Slovakia).

Laundering one's own illicit funds (c.1.6)

54. Though Section 231 explicitly criminalises laundering of a thing obtained through a criminal offence committed by another person, Section 233 does not include such explicit reference to self-laundering. *"Transfers to himself"* may not always mean covering self-laundering. A person might

transfer to himself a property that is obtained from a crime which was committed by others e.g. while assisting a person committing the predicate offence or money laundering offence. However, the evaluators accepted the Slovak authorities' claim that the phrasing in Section 233, which begins with the words *"Any person who performs any of the following..."* is widely understood by the courts to include the offender himself and therefore to cover "self-laundering". Therefore, self-laundering is criminalised under Section 233 of the SCC, although not under Section 231.

Ancillary offences (c.1.7)

55. C.1.7 requires that there should be appropriate ancillary offences to the offence of money laundering, including association with or conspiracy to commit, attempt, aiding and abetting, and counselling the commission, unless this is not permitted by fundamental principles of their domestic law. Evaluators consider that these ancillary offences are covered in Sections 13-14 and 19-21 of the SCC, in conjunction with Sections 233-234 of the SCC. Furthermore, conspiracy to commit money laundering is also criminalised in Section 13 of the SCC. 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 SCC including Article 296.

Additional element – If an act overseas which does not constitute an offence overseas but would be a predicate offence if occurred domestically leads to an offence of ML (c.1.8)

56. Section 4 of the SCC provides that criminal liability according to the SCC applies to acts committed outside the Slovak Republic when they are committed by a Slovak national or a foreign national with permanent residency status in the Slovak Republic. Based on this, the offences of "sharing" and "legalisation of the proceeds of crime" can be extended to offences committed overseas based on personal applicability, but in all other cases, paragraph 1 of Section 6 of the SCC applies and dual criminality is required, so that money laundering on the basis of the wider notion of predicate offences is not available in Slovakia.

Recommendation 2 (rated PC in the 3rd round MER)

Liability of natural persons (c 2.1)

57. As mentioned above, Section 233 of the SCC is the money laundering offence. This section applies to "any person who performs…obtained by crime…with the intention". The Slovak authorities advised that Section 233 of the SCC in addition to Sections 15 and 17 of the SCC comply with the c.2.1. Per Section 17, all offences are assumed to require intent as defined by Section 15, unless explicitly provided. So Section 231 of the SCC would also require intent. It can be concluded that the new provision covers all necessary intentional elements.

The mental element of the ML offence (c 2.2)

58. Criterion 2.2 requires that the law should permit the intentional element of the offence of money laundering to be inferred from objective factual circumstances.

59. The Slovak authorities advised that Sections 233 and 234 of the SCC (defining the money laundering offences) do not state that the offences could be committed by negligence and it means that an intention is required.

60. Under Section 17 of the SCC, “an act committed by a natural person shall involve criminal liability only in case of intentional causation, unless it is explicitly stated in this Act that causation by negligence is sufficient.”

31. Under Section 15 of the SCC:

"Intentional criminal offences are those where the offender

a) acting in a manner defined in this Act, had the intent to infringe or prejudice an interest protected under this Act, or

b) was aware that his act was likely to cause such infringement or prejudice and was prepared to accept that consequence should it occur."

61. These provisions do not explicitly make it possible to draw inferences from objective factual circumstances to provide the intentional element. Furthermore, no guidance as recommended by MONEYVAL in the 3rd round MER has been issued so far.

62. Slovak authorities provided the evaluators with the two Supreme Court judgments (R 19/1971 and R 60/1972). Furthermore, the representatives of the Prosecutors` Office indicated that this opinion is common to all prosecutors. The evaluators also examined the Judgment of the District Court in Prievidza (case no. 1T 110/2007) which convicted, *inter alia*, according to paragraph 1(a) and 2(b) of Section 233 of the SCC. In that case, one defendant was convicted of money laundering for repurchasing stolen cars, based on the fact that efforts were made to disguise the nature of the vehicles, including modifying VIN numbers and dismantling the vehicles before purchase and the others were convicted of sharing pursuant to paragraph 1(a) of Section 231 of the SCC. Although these decisions contain no explicit discussion of the *mens rea* required, based on their outcomes, the evaluators conclude that in criminal proceedings in practice it is possible to infer the intentional element of the ML offence from objective factual circumstances.

Liability of legal persons (c 2.3) Liability of legal persons should not preclude possible parallel criminal, civil or administrative proceedings (c 2.4)

63. One of the deficiencies identified in the 3rd round MER was the lack of criminal, civil or administrative sanctions for ML offences applicable to legal persons.

64. Slovakia, with the enactment of the Act no. 224/2010 Coll. amending the Criminal Code, has introduced what may be regarded as a form of criminal liability for legal persons to the Slovak legal system. The amendments that came into force on the 1st September 2010 have made it possible to impose protective/security measures on legal entities and confiscation of a property belonging to a legal entity.

65. Sections 83a & 83b of the SCC (See Annex V) now enable the courts to impose monetary sanctions if the criminal offence is committed under certain circumstances, while the court considers, *inter alia*, the seriousness of the committed criminal offence and additional elements as specified in Sections 83a & 83b of the SCC. However, it should be noted that according to Section 83a, the court might impose the confiscation of a sum of money in an amount of €800– €1,660,000.

66. Sections 83a & 83b of the SCC could be regarded as criminal liability as it is regulated in the SCC, applied in criminal proceedings by the Courts by taking into account the seriousness of the criminal offence, circumstances of the commission of the criminal offence and consequences for the legal person. However, it is recommended that the Slovak authorities review the confiscation limitation of €1,660,000, which could in some cases limit the range of confiscation of money (for instance in financial institutions accounts).

67. Since only criminal form of sanctions (confiscation) is relevant to legal persons, c.2.4 does not appear to be relevant in Slovakia.

Sanctions for ML (c 2.5)

Natural persons

68. According to Section 233 of the SCC, the court may impose on natural persons an imprisonment from 2 to 20 years. More specifically, the basic offence of legalisation of proceeds of crime carries a penalty of 2 to 5 years` imprisonment. The sanction could be increased to 3 to 8 years if the offender had a specific motivation or obtained larger benefit for himself or another through its commission. If the offender is a public figure, obtains substantial benefit, or acts in a more serious manner, the sanction increases to an imprisonment from 7 to 12 years. Finally, the penalty increases to from 12 to 20 years if the offender obtains large-scale benefit for himself or another, if the offence is related to trafficking in narcotics, psychotropic substances, nuclear or high risk chemical substances, weapons, or human beings, or to another particularly dangerous felony, or if the offender commits the offence as a member of a dangerous grouping. Forfeiture of the property, forfeiture of a thing or pecuniary penalty may be imposed along with the imprisonment. The court is not allowed to impose forfeiture of property along with the forfeiture of a thing or pecuniary penalty.

69. Sanctions under Section 231 of the SCC also vary based on a number of factors. Specifically, the basic offence of concealing, transferring, leasing or accepting property obtained by another's criminal offence or procured in exchange for such property, is liable to a term of imprisonment of up to 3 years. If the offender obtains larger benefit for himself or another, had a specific motivation or uses the thing for his own business purposes, he is liable to imprisonment of 3 to 8 years. If he obtains substantial benefit for himself or another or acts in a more serious manner, the penalty increases to 7 to 12 years. Finally, if the offenders obtains large-scale benefit for himself or another, or acts as a member of a dangerous grouping, he is liable to 12 to 20 years imprisonment.

Legal persons

70. The court shall confiscate property of a legal person if the conditions listed in paragraph 1 of Section 83b of the SCC are fulfilled, i.e. that the property or part thereof were obtained by a crime or as proceeds of a crime related to exercising the right to represent, make decisions in the name of, or carry out the control within, the legal person or related to negligence concerning the supervision or due diligence within that legal person. If the court does not impose the confiscation of the property, it is obliged to impose the confiscation of a sum of money (€800 to €1,660,000), considering the seriousness of the offence, its extent, the benefit gained, the damage caused, the circumstances of the commission, and the consequences of the confiscation for the legal person.

71. The sanctions available for natural and legal persons appear to be proportionate and dissuasive. However, as elaborated below, their effectiveness cannot be determined in light of the incomplete data provided to the evaluators. In so far as legal persons are concerned there is no Slovak practice to date.

Recommendation 32 (money laundering investigation/prosecution data)

72. Section 27 of the new AML/CFT Act authorises the FIU to keep statistics covering, inter alia, the number of cases submitted by the FIU to law enforcement authorities, the number of persons prosecuted or convicted of legalisation of proceeds from criminal activity, the value of seized or confiscated property, and to publish a summary review of that statistical data in an annual report. The same section also authorises it, for the purposes of keeping statistics, to require public authorities to supply all necessary documents and information to the FIU. However, this obligation appears not to cover keeping of statistics relating to terrorist financing cases. According to the Slovak authorities, the Slovak FIU has an obligation to keep summary statistical data on any tasks that it performs under the AML/CFT law and to require that public authorities and obliged entities supply all documents and information necessary to keep such data (involving terrorist financing). The Slovak FIU plans to include information related to terrorist financing cases in its 2010 annual report. In addition, the Ministry of Justice keeps statistics on convicted persons pursuant to the

relevant provision, although there have been no terrorist financing convictions to date. Such statistics, in any case, would not include whether the original information was derived from the UTR system. In any case, in the absence of any cases of terrorist financing to date, the evaluators were unable to assess the effectiveness of the statistical data collection.

73. The Slovak Prosecution Service provided the following statistics with regard to money laundering investigations, prosecutions and convictions *(according to the Section 252 of the old SCC and Section 233 of the new SCC)* :

Table 6: Statistics on money laundering investigations, prosecutions and convictions (Section 252 old SCC and 233 of new SCC)

Year	Number of Investigated persons	Number of Prosecuted persons	Number of Convicted persons
2005	73	36	9
2006	57	37	10
2007	58	34	12
2008	33	18	10
2009	39	24	8
2010	41	25	13

74. The Slovak Prosecution Service provided the following statistics with regard to the offences of "sharing" offence under Section 231 and negligent ML offence under Section 232 of the SCC:

Table 7: Statistics on investigations, prosecutions and convictions (sharing offence under section 231 and negligent ML offence under 232 of the SCC)

Year	Number of investigated persons	Number of prosecuted persons	Number of convicted persons
2005	365	265	154
2006	235	120	150
2007	249	142	89
2008	231	121	85
2009	198	108	93
2010	210	117	103

Table 8: Statistics on negligent money laundering offence (Section 232)

Year	Number of Investigated persons	Number of Prosecuted persons	Number of Convicted persons
2005	7	3	0
2006	5	3	4
2007	5	1	2
2008	18	3	1
2009	11	2	4
2010	18	5	4

75. The Slovak authorities advised that from the practice of the public prosecution service, the most frequent predicate offences are car theft and economic offences, mainly fraud cases. From the Slovak authorities' perspective, drug-related offences are in decline as a link of money laundering, and there is still significant migrant smuggling and corruption.

76. On 24 November 2010, the Slovak Authorities provided the following statistics. The table hereinafter provides the statistical data of money laundering cases pursuant to the Section 233 of the SCC (and Section 252 of the SCC in force until 31 December 2005) for the period of 2005 until 31 October 2010 (based on examination of relevant dossiers kept in the Office of Special Prosecution, Military Prosecution Services and the district and regional prosecution services).

Table 9

	2005	2006	2007	2008	2009	2010	Total
Criminal prosecution	71	49	47	54	78	71	369
Prosecuted persons	57	25	28	22	39	25	195
Persons charged with a crime	19	5	19	7	12	10	72
Freezing measures1/value of frozen financial means in Euros	1/1.161.000	1/AB	1/416.978,22	1/5.000	1/5.000 1/10.000 13/70.244,55 1/13.000 1/3.000 1/875.035	1/3.761,47 1/234.308,49	11/ 2.797.32 7.73
Confiscation decisions2/value of confiscated financial means in Euros	1/VND		1/VND 1/30.000		1/T 1/T 1/electronics	2/T 1/C	9
Protective measures3					1/5xC 2/C	1/34.290,55 1/C	5
Number of measures – other method of freezing/seizure of a thing for the purposes of criminal proceedings4	C -14 T -5x M - 3000 €	C – 25 M : - 763.730,-SK, - 21.685-€, - 5.000-CZK, -10.000,-USD Other things -1	C -17 Other things - 1	C – 29 M - 5100 €	C – 67 Ship engine – 10x Construction engineering – 2x groceries - 1/26.000 € electronics and cars – 1/145.063,92€ Construction engineering	C – 42	

[1] – Section 95, Code of Criminal Procedure
[2] - Section 58, 60 Criminal Code
[3] - Section 83 s., Criminal Code
[4] - Section 89, 92, 93 of the CPC – things handed over voluntarily for the purposes of criminal proceedings or things secured pursuant to separate laws (e.g. Act on Police Forces) – rendered back to the owner after criminal proceedings
(C- cars and motorcycles, T- Tobacco and cigarettes, M – Money, AB – Account Balance, VND-the value of things can not be determined)

77. The Slovak Authorities provided a breakdown of the predicate offences which served as the basis of the money laundering offences as follows:

Table 10

	2005	2006	2007	2008	2009	2010	Total
Car theft	35	30	13	72	40	102	292
Unauthorised use of motor vehicle belonging to another	3		1			1	5

Theft of other things or documents	4	5	4	4	11	9	37
robbery		1			1		2
Embezzlement and fraud	7	8	6	5	10	6	42
Computer fraud			1	1	3	1	6
Procuring prostitution			2	1	1		4
Breach of regulations governing imports and exports of goods – Section 124	16	1				1	18
Tax and insurance evasion or failure to pay tax and insurance	7		10	1	8	1	27
Establishing, conspiring and supporting criminal group			10		8		18
Breach of regulations on state technical measures to mark goods	4	3			1		8
Abuse of powers of public official		2					2
Illegal gambling		1					1
Criminal acts related to unauthorised possession and trafficking in narcotic substances and precursors	2		1				3
Unlawful business activities					2		2
Unauthorised possession of firearms and trafficking in them	1						1
Breach of copyright	1						1
Poaching	1						1
Smuggling of people				1			1
total	81	51	48	85	85	121	471

78. Regarding the statistics presented above, it should be noted that several different sets of statistics were presented to the evaluators in the course of the evaluation, each of which was represented as being up-to-date and accurate. Furthermore, the authority that provided the latest set of statistics, a branch of the public prosecutor's office, was unable to explain who had provided the prior statistics (which were also from the public prosecutor's office) or the nature of the statistics themselves. In addition, inconsistencies between the various tables, even as provided most recently, lead to serious concerns that the manner of calculating these statistics is not fully coherent. Although evaluators are convinced that there have been indictments and convictions for the money laundering and sharing offences, the above facts make it difficult for evaluators to regard the statistics as clear indications of the actual scope of legal proceedings.

Effectiveness and efficiency

79. The Slovak authorities explained that legalisation of proceeds from crime against property has been the most frequent form of money laundering **in particular from car theft**. Alteration/modification of identification elements of stolen cars has been the typical method of commission of this kind of crime, and therefore also forgery of documents and subsequent sale of legalised vehicles. Comparing data in car registers or catching a car sought on state borders, mostly between Slovakia and Ukraine, has been the most frequent method of discovering this kind of criminal activity. The majority of vehicles originated from car thefts committed outside Slovak territory, especially in Italy, Austria, Germany, Belgium and Czech Republic whilst the majority of cars have been

registered in SIS. Knowledge acquired by prosecuting and adjudicating authorities in the course of other criminal proceedings and/or from securing measures (home searches, searches of other premises) has been the second most frequent grounds for commencement of criminal prosecution of this kind of criminal activity. Individual cars have been subject matters of majority of cases. Multiple car thefts and/or extensive cases represented 5 to 7% of caseload.

80. The statistics provided prove that car theft is the major proceeds generating offence in the Slovak Republic, where Sections 231 and 233 of the SCC are frequently prosecuted in the same proceedings as the predicate offence.

81. The Prosecutor's Office stated that there is no impediment to convicting a person for money laundering without conviction for the predicate offence.

82. Although most of the essential criteria in Recommendations 1 and 2 appear to be formally met, there are concerns about the implementation of the money laundering tools with regard to criminal activity.

83. The statistics present a low number of convictions and agreements on guilt and punishment. Furthermore, the offence of car theft, which in many jurisdictions would generally be treated as a receiving offence, is the predicate offence at no less than 62% of the money laundering cases, since in total 292 out of 471 cases were linked to car theft. Furthermore, theft of other things or documents consists of 37 cases in total, which increases the offences treated as receiving offences to 70% of the money laundering cases.

84. These statistics show clearly that prosecutions of crimes of these types are not the primary goal of the AML regime and it seems that the use of the money laundering offence is not used effectively in a wider range of more serious predicate offences.

2.1.2 Recommendations and comments

Recommendations 1, 2 and 32

85. Though most of the essential criteria under Recommendations 1 and 2 appear to be formally met, it seems that the definition of "property" does not fully comply with the Methodology. Therefore, Slovak authorities should define "property" in accordance with the FATF Methodology.

86. It is noted from paragraph 45 of the report that there is a significant threat from domestic organised crime investing its proceeds in the domestic economy. From the criminal statistics provided for 2009 alone there were 352 convictions for participation in organised criminal groups and racketeering, 1,079 convictions for drug trafficking, 4,182 convictions for fraud. There were at least 15,634 convictions for proceeds-generating cases generally. It is against this background that the evaluators have looked at the quality of the money laundering cases being brought forward and which have resulted in convictions. The majority of the predicate offences relate to car theft/disguise of cars – which in most other jurisdictions would be unlikely to be the subject of money laundering charges at all, but would be dealt with through receiving/handling offences. There is no evidence of money laundering prosecutions or convictions in relation to the major and more serious proceeds-generating cases perpetrated by organised crime or others for pure economic gain. In these circumstances there is little or no evidence that has been seen by the examiners which indicates that money laundering investigation and prosecution of money laundering is being used seriously as a tool to combat the organised crime threat. The statistics do not show how many convictions relate to third party laundering on behalf of others, as opposed to self-laundering, or indeed, how many cases were generated by the police through the financial investigations in parallel with their investigations into the predicate offences. The continued lack of effective use of

money laundering as a tool to fight proceeds-generating crime, especially in respect of autonomous third party laundering cases, was very disappointing.

87. The Slovak authorities should analyse the reasons for the apparent discrepancy between the extent of the organised crime in Slovakia and the quality of ML cases brought forward and which have resulted in convictions. They should further assess the reasons of the ineffective use of ML investigation and prosecution as a tool to combat organised crime and major proceeds generating offences. In the light of these assessments Slovak authorities should take further appropriate steps including awareness raising activities for the police, prosecutors and judges.

2.1.3 Compliance with Recommendations 1 and 2

	Rating	Summary of factors underlying rating[4]
R.1	**PC**	• The definition of "property" is not sufficiently clear and the ML offence does not clearly extend to the indirect proceeds of crime. • Not all designated categories of offences are fully covered as predicates, as there is no full criminalisation of financing of individual terrorists' day-to-day activities or of the financing of the acts defined in the treaties annexed to the UN TF Convention. • There is insufficient evidence of effective implementation.
R.2	**C**	

[4] Note to assessors: for all Recommendations, the description and analysis section should include the analysis of effectiveness and should contain any relevant statistical data

2.2 Criminalisation of Terrorist Financing (SR.II)

2.2.1 Description and analysis

Special Recommendation II (rated NC in the 3rd round MER)

Legal framework

88. Special Recommendation II was rated *"Non-Compliant"* in the 3rd round MER and it was recommended that the Slovak authorities should introduce as a matter of urgency an autonomous offence of TF, which explicitly addresses all the essential criteria under SR II, and the requirements of the Interpretative Note. The evaluation team welcomed the amendments made to SCC that came into force on 1 January 2010 and introduced an autonomous offence into Slovak law. When Sections 129, 297 and 419 are interpreted together, it seems that Slovak TF offences are mostly in line with the requirements of both the TF Convention and the FATF standards. However, a number of shortcomings still prevent the Slovak TF offences from being fully in line with the requirements of SR II.

Criminalisation of financing of terrorism (c.II.1)

89. The TF offence is defined in Section 419 of the Criminal Code. Articles 129 and 297 of the SCC complements the TF therefore Section 419 should be read in conjunction with these sections when analysing TF offences. Act No. 576/2009 Coll. on amendment of the Criminal Code entered into force on 1 January 2010. This Act changed the wording of the Section 419, which criminalises any act intended to cause death or serious bodily injury to a civilian, when the purpose of such act is to intimidate a population or to compel a government or an international organisation to do or to abstain from doing any act. It also incriminates others forms of the participation on commission of those acts including by financing.

90. The first paragraph of Section 419 reads as follows:

(1) Who

*a) with an intent to seriously intimidate inhabitants, seriously destabilise or defeat constitutional, political, economical or social establishment of **the state** or a structure of an international organisation, or to coerce a government of **the state** or an international organisation to act or to omit to act, threats by commitment or commit an offence endangering the life, health of people, their personal freedom or a property, or illegally produces, gets, owns, possesses, transports, delivers or in another way uses explosives, nuclear, biological or chemical weapons, or performs not permitted research and development of such weapons or weapons prohibited by law or by an international treaty,*

b) with the intent to cause death or serious bodily harm or considerable damage on property or environment possesses radioactive material, or has or creates nuclear explosive machine or a machine diffusing radioactive material or emanating radiance, which may due to its radiological features cause death, serious bodily harm or serious damage on property or environment, or

c) with the intent to cause death or serious bodily harm or considerable damage on property or environment, or to coerce natural person or legal person, international organisation or state to act or omit to act, uses radioactive material or nuclear explosive system or a system diffusing radioactive material or emanating radiance which may cause death due to its radiological features, or serious bodily harm or considerable damage on property or on environment, or

uses or damages a nuclear reactor including reactors installed on floats, vehicles, planes or cosmic objects, used as an energy source for driving such floats, vehicles, planes or cosmic objects, or for other purposes, or premises or traffic system used for production, storage, processing or transport of radioactive material in a manner which releases or may release radioactive material, or threats by such act in circumstances indicating credibility of the threat, or

d) asks for radioactive material, nuclear explosive system or system diffusing radioactive material or emanating radiance which may due to its radiological features cause death, serious bodily harm or considerable damage on property or environment, or a nuclear reactor including reactors installed on floats, vehicles, planes or cosmic objects used as an energy source for driving such floats, vehicles, planes or cosmic objects or for other purposes, or premises or traffic system used for production, storage, processing or transport of radioactive material, with threats in circumstances indicating credibility of the threats or use of power,
shall be imposed an imprisonment sentence for 20 to 25 years or life imprisonment.

…..…

(3) The life imprisonment shall be imposed on the offender if s/he commits the act listed in the paragraph 1

e) and gives rise a serious bodily harm to more persons or death of more persons,
f) on a protected person,
g) towards armed forces or armed corps,
h) as a member of a dangerous grouping, or
i) during a crisis situation."

91. According the Slovak authorities, the term "the State" in the above section includes offences committed against any state in the world, and not only against the Slovak Republic, as express wording would be required to limit the scope of the section. Though Article 419 does not explicitly name these acts as terrorist acts, taking into account the title of the Section it can be concluded that Slovakia criminalises terrorist acts in the meaning of Interpretative Note.

92. According to Section 297 of the SCC, *"Any person who establishes or masterminds a terrorist group, is its member, actively participates in it or supports it shall be liable to a term of imprisonment of eight to fifteen years."* For the purposes of the SCC, the term "terrorist organisation" is defined under paragraph 5 of Section 129 of the SCC as *"a structured group of at least three persons existing for a certain period of time with the objective of committing the offences of terror and terrorism"*.

93. The second paragraph of Section 419 of the SCC defines TF offences as follows:

"(2) The same sanction as in the paragraph 1 shall be imposed to the person who

a) collects or provides financial or other means, personally or through another person, even partially, for the purposes of their use or allowing their use for commitment of the act listed in paragraph 1,

….

(4) The life imprisonment shall be imposed to the offender if she/he commits the act listed in the paragraph 2 letter a) and herewith facilitates using the financial or other sources collected or provided by him, for committing the attempt of the offence listed in the paragraph 1, or s/he personally uses them in such manner, or commits the act listed in the paragraph 2 letter d) and herewith allows commitment or attempt of the act listed in the paragraph 1."

94. Paragraph 7 of Section 129 of the SCC defines supporting a terrorist group as *"an intentional action consisting in providing financial or other means, services, and co-operation, on in creating other circumstances serving the purpose of*

a) establishing or maintaining the existence of such a group;
b) *committing, by such a group, the criminal offences referred to under paragraph 3 or 4."*

95. Paragraph 2 of Section 419 of the SCC criminalises the provision or collection of financial or other means, directly or indirectly, for the purpose of their full or partial use to carry out acts mentioned in the first paragraph of the same section. Therefore, the evaluators conclude that the Slovak law incriminates TF offence fully in line with paragraph 1(b) of Article 2 of the UN TF Convention. However, the prohibition of financing terrorism, as defined in Section 419 (2), does not cover financing of all the acts as mentioned in the treaties listed in the annex of the UN TF Convention. The UN TF Convention requires that financing of the acts that constitute offences within the scope of as defined in the following conventions be considered as the financing of terrorism: the Convention for the Suppression of Unlawful Seizure of Aircraft, the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, the Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, the International convention against the Taking of Hostages, the Convention on the Physical Protection of Nuclear Material, the Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf and the International Convention for the Suppression of Terrorist Bombings. Although the acts included in these conventions are themselves criminalised under the Criminal Code, Section 419 (2) defines the terrorist financing offence narrowly, limiting itself to the offences delineated in Section 419 (1). For example, the Convention for the Suppression of Unlawful Seizure of Aircraft creates an offence of unlawfully seizing an aircraft by force or threat thereof and the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation creates an offence against unlawfully performing acts of violence against persons on an aircraft is said act is likely to endanger the safety of the aircraft; these acts are criminalised under Section 291 of the SCC. Similarly, the International Convention against the Taking of Hostages forbids detaining any person in order to compel a third party to take some action; this offence is covered under Section 185 of the SCC. However, the issue here is not the incrimination of the acts themselves, but the criminalisation of financing of these acts as the offence of financing of terrorism. The wording of Section 419(2) refers **only** to one who "collects or provides financial or other means... for the purposes of their use or allowing their use for the commitment of the act listed **in paragraph 1**". Therefore, "financing of some of the acts" found in the treaties listed in the Annex to the UN TF Convention is **not** criminalised under the SCC.

96. It is clear that Section 419 of the SCC does not criminalise financing of terrorist organisations or an individual terrorist for the purposes other than the acts mentioned in paragraph 1 of the same section. However, Section 297 when read in conjunction with Section 129 of the SCC can be interpreted as criminalising financing of a terrorist organisation's day-to-day activities other than the acts mentioned in paragraph 1 of Section 419 of the SCC. Though Section 297 of the SCC incriminates membership of a terrorist organisation, the evaluators conclude that the Slovak law does not criminalise financing of an individual terrorist's day-to-day activities other than the acts mentioned in paragraph 1 of Section 419 and other than according to Section 339, as required under criterion II.1.

97. As there have not been any investigations, prosecutions or convictions for the offences of terrorist financing the interpretation or implementation of Sections 129, 297 and 419 have not yet been tested in Slovakia.

98. The Slovak law does not provide a definition of "financial or other means". Although Slovak authorities claim that the term covers all types of assistance, the wording of this phrase, which places an emphasis on financial means, leads to concerns that certain types of funds, such as legal

documents as included in the definition of funds in the FATF Glossary of definitions used in the methodology, might not be fully covered. However, in the course of the pre-meeting the Slovak authorities drew the attention of the evaluators to the formal and statutorily recognised interpretation of Article 1/1 of the TF Convention (Act No 593/2002 Coll.). Taking that text into account in conjunction with Article 7 of the SCC the evaluators were satisfied that there was a reasonable expectation that the courts would interpret the statutorial language in a manner consistent with international standards.

99. Criterion II.1(c) of the Methodology states that TF offences should not require that the funds (i) were actually used to carry out or attempt a terrorist act(s); or (ii) be linked to a specific terrorist act(s). There is no explicit provision in the Slovak SCC that indicates the compliance of Slovak SCC with this provision. However, Section 419(2) of the SCC refers to providing funds "for the purposes of their use or allowing their use for commitment of the act listed in paragraph 1". This might indicate that the financing offence must be linked to a specific act. Therefore, as detailed above, it does not seem that this criterion is met.

100. Attempt is criminalised for all offences including terrorist financing offences according to the general criminal law principles in Slovakia as set forth in Sections 13 and 14 of the SCC. The common ancillary offences (see above for ML) are also applicable in the TF context.

Predicate offence for money laundering (c.II.2)

101. According to the provisions of the SCC, the predicate offence of ML can be any crime. Since funding of an individual terrorist's day-to-day activities is not fully criminalised under Slovak law in line with SR II, only the offences of financing of terrorist acts and terrorist organisations are predicate offences for money laundering.

Jurisdiction for Terrorist financing offence (c.II.3)

102. As there is no limitation in the SCC in this regard, evaluators believe that the TF offences are applicable regardless of the location of the terrorist group or irrespective of the place where the terrorist act is, or is planned to be committed.

The mental element of the FT (applying c.2.2 in R.2)

103. The abovementioned provisions relating to TF offences or any other provision in the SCC do not explicitly make it possible to draw inferences from objective factual circumstances to provide the intentional element. As noted above under R.2, the evaluators are of the opinion that in criminal proceedings in practice it is possible to infer the intentional element of the TF offences from objective factual circumstances.

Liability of legal persons (applying c.2.3 & c.2.4 in R.2)

104. As noted above under Recommendation 2, Slovakia with the enactment of the Act no. 224/2010 Coll. amending the Criminal Code has introduced criminal liability for legal persons to the Slovak legal system. The criminal liability applies to TF offences as well. The sanctions available for natural and legal persons for TF offences appear to be proportionate and dissuasive. However, as there has been no conviction so far for TF offences their effectiveness in practice could not be determined by the evaluators.

Sanctions for FT (applying c.2.5 in R.2)

105. The penalty under paragraph 2 of Section 419 of the SCC for financing of terrorist acts is 20 to 25 years imprisonment. A more severe sanction of life imprisonment is also possible in certain cases, as specified in paragraphs 3 to 4 of Section 419. The sanction for financing a terrorist organisation for any purposes other than terrorist acts under Section 297 of the SCC is 8 to 15 years

imprisonment. The sanctions regime appears to be proportionate and dissuasive. However, the absence of any sanctions in practice gives rise to concerns regarding the implementation of this procedure, and as a result raises effectiveness issues.

Recommendation 32 (terrorist financing investigation/prosecution data)

106. As noted above, Section 27 of the new AML/CFT Act authorises the FIU to keep statistics covering, inter alia, the number of cases submitted by the FIU to law enforcement authorities, the number of persons prosecuted or convicted of legalisation of proceeds from criminal activity, the value of seized or confiscated property, and to publish a summary review of that statistical data in an annual report. The same section also authorises it, for the purposes of keeping statistics, to require public authorities to supply all necessary documents and information to the FIU. Though this obligation under Section 27 does not cover the keeping of statistics relating to terrorist financing cases, the authorities report that the FIU, in practice, collects statistics on the disseminated information related to terrorist financing. However, as noted above, according to Slovak authorities, the Slovak FIU and the Ministry of Justice keep certain statistics on their work, including information on convictions. Even if this is the case, given the lack of investigations, prosecutions and convictions for terrorist financing to date, the evaluators were unable to assess the effectiveness of the statistical data collection and are left with concerns over the consistency of the system for keeping statistics, as noted above.

Effectiveness and efficiency

107. At the time of the on-site visit, there had been no investigations, prosecutions and convictions for TF offences in Slovakia. For this reason, the existing legislative framework has not yet been tested in practice. However, after the on-site visit the Slovak authorities informed the evaluators of the existence of an ongoing prosecution in 2010 pursuant to Section 297 of the SCC. However, evaluators were not provided with any statistics on the efficiency of prosecution under Section 419 of the SCC generally or 419(2) specifically, and the evaluators understand that no such investigations and prosecutions have taken place.

108. During the discussions held with the Counter-Terrorism Unit of the Bureau of Combating Organised Crime on-site, one case was mentioned relating to transfer of money linked to a designated person according to UN Resolution 1267. However, the police specified that this was intelligence information and no police investigation resulted from it. The Slovak Information Service was not informed of the case.

109. The absence of any terrorist financing cases gives rise to concerns that the Slovak authorities may be insufficiently focused on the significance of investigating and prosecuting terrorist financing cases. Furthermore, the evaluation team formed the impression that there was ample scope for improved co-ordination between the competent authorities in this important sphere.

2.2.2 Recommendations and comments

Special Recommendation II

110. The financing of individual terrorist's day-to-day activities should be criminalised as required by criterion II.1.

111. The SCC should be revised to ensure proper criminalisation of financing of the acts arising from the Convention by amending Section 419 (b) so that it covers financing of offences under the other sections of the SCC criminalising the acts pursuant to the treaties listed in the annexes to the UN TF Convention.

Recommendation 32

112. Section 27 of the new AML/CFT Act should be amended to authorise the FIU to keep statistics on TF offences.

2.2.3 Compliance with Special Recommendation II

	Rating	Summary of factors underlying rating
SR.II	**PC**	• No full criminalisation of financing of an individual terrorist's day-to-day activities. • Non-criminalisation of the financing of the acts defined in the treaties annexed to the TF Convention. • Effectiveness concerns.

2.3 Confiscation, Freezing and Seizing of Proceeds of Crime (R.3)

2.3.1 Description and analysis

Recommendation 3 (rated PC in the 3rd round MER)

Legal framework

113. Recommendation 3 was rated *"Partially Compliant"* in the 3rd round MER on the grounds that there were some concerns about the legal structure of the seizure and freezing regime to ensure that all indirect proceeds, substitutes etc may be liable to confiscation in due course and the laws did not clearly provide for forfeiture from third parties and for the protection of bona fide third parties. The absence of any clear authority to take steps to prevent or void actions as required by essential criterion 3.6 was another underlying factor for that rating. In addition, the evaluators of the 3rd round had doubts about the effectiveness of the legal regime's effectiveness especially taking into account the lack of any property forfeited in ML cases as at the time that evaluation.

114. The new SCC that came into force in January 2006 established a new legal framework for the forfeiture/confiscation of the proceeds of crime. (Sections 58-60 and 83 of the SCC) While this is generally in line with relevant international standards, some issues remain.

Confiscation of property (c.3.1)

115. Forfeiture is primarily governed by Sections 58 to 60, whilst the confiscation of a thing is regulated under Section 83 of the SCC.

116. Section 58 of the SCC lays down the conditions for "forfeiture of property" of an offender where he/she gained or tried to gain large-scale property benefits or caused large-scale damage, as well as where the offender has acquired his/her property or part thereof from the proceeds of crime at least to a substantial extent. According to first paragraph of this Section, the court may order the forfeiture of property of the offender whom it sentences to life imprisonment or to unconditional imprisonment for a particularly serious felony, through which the offender gained or tried to gain large-scale property benefits or caused large-scale damage. As understood from the wording of this paragraph, the power of forfeiture of property of an offender under these circumstances is a discretionary one. However, the power granted to courts under the second paragraph is mandatory. According to the second paragraph of Section 58 the court shall order the forfeiture of property,

even in the absence of the conditions referred to in the first paragraph, when sentencing perpetrators of certain proceeds generating criminal offences listed therein including ML and TF offences, if the offender has acquired his property or part thereof from the proceeds of crime at least in the substantial extent. However, it should be noted that the second paragraph of Section 58 came into force on the 1st September 2010. The evaluators, therefore, could not assess the effectiveness of this new provision.

117. In turn Section 60 of the SCC sets out the "forfeiture of a thing". The first paragraph of this section reads:

"(1) The court shall order the forfeiture of a thing, which was
a) used to commit a criminal offence,
b) intended to be used to commit a criminal offence,
c) obtained by means of a criminal offence, or as remuneration for committing a criminal offence, or
d) obtained by the offender in exchange for a thing referred to in c).

118. According to the second paragraph of Section 60, if the thing referred to in paragraph 1 is inaccessible or unidentifiable, or is merged with the property of the offender, or with the property of another person obtained by lawful means, the court may impose the forfeiture of a thing whose value corresponds to the value of the thing referred to in paragraph 1. The third paragraph further defines "an inaccessible thing". (for the definition see Annex V) However, the power of forfeiture of a thing whose value corresponds to the value of the thing, where the thing is inaccessible or unidentifiable, seems not to be mandatory.

119. Paragraph 4 of Section 60 further enlarges the meaning of "thing" by stating that *"a thing within the meaning of paragraph 1 shall also mean the proceeds of crime, as well as profits, interests, or other benefits arising from such proceeds or things"*.

120. The examiners were advised that in Slovak jurisprudence "proceeds" means anything that has been obtained by a criminal offence or is closely connected with it.

121. Section 83 of the SCC regulates "confiscation of a thing" in the case that the sanction of forfeiture of a thing referred to in paragraph 1 of Section 60 of the SCC was not imposed. Confiscation of a thing, which is also mandatory, could be applied under the following circumstances;

a) if it belongs to the person who cannot be prosecuted or sentenced,
b) if it belongs to the offender whose punishment the court waived, or the offender whose prosecution was stayed, or the offender whose prosecution was conditionally stayed, or the offender whose prosecution was stayed due to the conclusion of a conciliation agreement,
(c) if it consists of goods that are not marked with control stamps or goods that were not subjected to other technical control measures required by generally binding legal acts for taxation purposes,
(d) if the circumstances of the case justify the presumption that the thing could be used as a source to finance terrorism, or
(e) if this is necessary with regard to the security of people or property or other similar general interest.

122. This sanction shall not be applied according to the third paragraph of Section 83, if:
- the injured party is entitled to the compensation for damage caused by the offence, which the confiscation of the thing would render impossible, or
- the value of the thing is manifestly disproportionate to the gravity of the minor offence.

123. The evaluators conclude that these provisions provide for the confiscation of property that has been laundered or which constitutes proceeds from, instrumentalities used in and instrumentalities intended for use in the commission of ML, TF and other predicate offences and property of corresponding value as required under essential criterion c.3.1.

124. However, there is not any explicit indication that extends the property to the indirect proceeds of money laundering offences as required under essential criterion c.3.1.1 (a).

125. Slovak law still does not allow the forfeiture or confiscation from third parties except the offender's property that merged with the property of a third party. It is explicitly mentioned in Section 60 that the court may impose the sentence of forfeiture of a thing only if the thing belongs to the offender. However, Section 83 of the SCC permits confiscation of an object when it belongs "to the person who cannot be prosecuted or sentenced." According to Slovak authorities, this Section was amended in 2006, so that it referred to any person and not only "the offender who cannot be prosecuted or sentenced". Although no case law was brought indicating that this section is interpreted to allow confiscation from innocent third parties, the Slovak authorities provided a decision from 1971 to show that third party forfeiture was possible. Based on this decision, as well as the amendments to Section 83, the evaluators accepted the Slovak authorities' claim that third party confiscation was possible under the law. However, it should be noted that during the on-site visit, Slovak authorities indicated that offenders could avoid confiscation by transferring property to third parties, indicating that third-party forfeiture is not, practically, an option. Since the amendment of the Criminal Code (Act no. 224/2010 Coll.) which introduced corporate liability, the provisions of Section 83 par. 1 (a), (c), (d) and (e) might be applied on things that belong to a legal person. However, this has not yet been confirmed in practice. In any case, the provisions of par. 1(b) cannot be applied to legal persons due to exact definition of the offender in the Section 19.

Provisional measures to prevent any dealing, transfer or disposal of property subject to confiscation (c.3.2) Initial application of provisional measures ex-parte or without prior notice (c.3.3) Adequate powers to identify and trace property that is or may become subject to confiscation (c.3.4)

126. Section 95 of the Code of Criminal Procedure states:

Seizure of financial assets

(1) If facts indicate that financial assets on an account in a bank or branch of a foreign bank or other financial assets are dedicated to committing a criminal offence, they were used to commit a criminal offence or they are proceeds of a crime, president of a panel of judges and a prosecutor in the preliminary stage may order to seize the financial assets. The order to seize under the first sentence may concern also financial assets additionally accrued at the account, including ancillary rights, if the reason of the seizure refers also to them.

(2) If the case disallows a delay, prosecutor may order according to the paragraph 1 even before the beginning of criminal proceedings. Such order shall be confirmed by a judge for the preliminary proceedings in 48 hours at the latest otherwise it becomes invalid.

(3) The order shall be issued in written and shall be reasoned. In the order the sum in the relevant currency which the order refers to, shall be included as far as it can be enumerated in the time of the decision. In the order any disposition with the seized financial assets up to the indicated sum shall be prohibited unless the president of the panel of judges and the prosecutor in the preliminary proceedings decide otherwise.

(4) Seizure shall not include the financial assets which are necessary to satisfy requisite needs of life of the accused person or a person, of which the upbringing or subsistence the accused or the person of which the financial assets were seized, is obliged to take care.

(5) If the seizure of the financial assets is not necessary any more for the purposes of the criminal proceedings, it shall be set aside. If it is not necessary in the stipulated amount, the seizure shall be reduced. The president of the panel of judges and the prosecutor in the preliminary proceedings shall decide by an order about the setting aside or reduction of the seizure.

(6) The order according to the paragraph 1 or 2 shall be always delivered to the bank, branch of a foreign bank or another legal person or natural person who disposes of the financial assets, and after the realisation of the order even to the person whose financial assets were seized.

(7) The seized financial assets may be disposed of only upon previous accord of the president of the panel of judges and prosecutor in preliminary proceedings. While the seizure is running, all legal acts and claims for the seized financial assets are ineffective.

(8) The person, whose financial assets were seized, is allowed to ask for setting aside or reduction of the seizure. The president of the panel of judges and prosecutor in the preliminary proceedings shall decide on such application without delay. Against such decision a complaint may be lodged. If the complaint was dismissed, the person whose financial assets were seized is allowed to lodge it again without giving new reasons after the lapse of 30 days since the decision on the previous complaint entered into force; otherwise it shall not be dealt with.

(9) If it is necessary to seize the financial assets in the criminal proceedings to assure the claim for damages of the victim, paragraphs 1 to 8 shall be applied mutatis mutandis.

127. There are additional powers under Sections 113, 114, and 551 of the CCP, all of which provisions seem to cover the relevant requirements.

128. Under Section 95 of the CCP, prosecutors may seize financial means prior to commencement of criminal prosecution, with the order requiring judicial approval within 48 hours. Such seizure is not limited to means generated from criminal activity, and can affect any bank account linked to the criminal act under investigation, even if it does not belong to the accused. Section 96 of the CCP allows the same mechanism for bonded securities.

129. Prosecutors have the power to issue orders to intercept and record telecommunication operations (Section 115 of the CCP) and to order video and sound recording (114 of the CCP). Both such orders require pre-trial judicial approval within 24 hours. In addition, under paragraph 5 of Section 113 of the CCP, a prosecutor or police officer may require authorised entities to grant them access to data subject to various legal secrecy protections. This power is granted to a prosecutor before or after commencement of criminal proceedings, and to a police officer within pre-trial proceedings and upon prior consent by a prosecutor.

130. Section 551 of the CCP gives the court power to provisionally seize property located in the Slovak Republic that was or is designated to be used for criminal activity or is generated from criminal activity, upon request by a foreign authority. In an urgent situation, a prosecutor has a right to issue this order, subject to approval by a judge within 48 hours. There is no requirement that such means belong to a person under criminal prosecution or accused of any crime.

Protection of bona fide third parties (c.3.5)

131. With regard to protection for the rights of bona fide third parties, Slovak authorities referred to Sections 45 to 50 of the CCP. However, Section 45 of the CCP is the only relevant section relating to this issue. Section 45 provides that any party whose thing was seized has the right to participate in the legal seizure proceedings, and other provisions of the CCP provide a variety of other procedural rights. Despite the claims of the Slovak authorities that the right to participate in legal proceedings qualifies as protection of substantive rights, the evaluators reached the conclusion that it would be difficult for the courts to grant any real remedy to the parties appearing before them without some legislative basis giving them a substantive right to such remedy. Although Slovak authorities provided that a party, who has registered a pledge or mortgage on a property, retains

those rights on the property in case of its seizure. If the pledge has not been registered, the injured party is allowed to bring an action to the competent civil court. The protection is provided by the civil court if the party is able to prove its legal claims. However, the protections given to parties with pledges on a property do not extend to those bearing other forms of rights, and no other evidence was provided to the evaluators to demonstrate any substantive remedy guaranteed to parties bearing said rights. Indeed, the fact that special protections are provided to parties with pledges may serve to highlight the fact that the procedural measures of the CCP are not sufficient to guarantee substantive rights and remedies, given that the legislator made sure to provide pledge-bearers with additional protections. In light of the above, the evaluators conclude that no positive substantive protections exist for parties with rights to a seized object, other than those bearing pledges or mortgages on a property.

Power to void actions (c.3.6)

132. The Slovak Republic has not taken any legislative steps to create a clear authority to take steps to prevent or void actions, where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in the ability to recover property subject to confiscation.

Additional elements (c.3.7)

133. Article 58(2) of the SCC allows forfeiture of property when sentencing offenders for a number of violations, if the offender has acquired his property or part thereof from the proceeds of crime at least in the substantial extent. One of the violations permitting such forfeiture is Section 296 of the SCC, the offence of establishing, masterminding and supporting a criminal organisation. However, this article allows forfeiture of the property of individuals convicted of this offence, rather than of the criminal organisation itself. Therefore, it seems that forfeiture of the property of a criminal organisation would be possible only under articles 83a and 83b of the SCC, if the organisation is a legal person.

134. Section 83 of the SCC regulates non-conviction based confiscation. According to this section confiscation of a thing could be applied, in the presence of other statutory requirements, if it belongs to the person who cannot be prosecuted or sentenced; if it belongs to the offender whose punishment the court waived, or the offender whose prosecution was stayed, or the offender whose prosecution was conditionally stayed, or the offender whose prosecution was stayed due to the conclusion of a conciliation agreement.

135. As at the time of the on-site visit there was no legal provision in force which regulates reversal of burden of proof. However, Slovakia appears to have introduced such legal concept into its legal system by the Act No. 101/2010 Coll of 4 March 2010 on the Proof of Origin of Property, which came into force on the 1st January 2011.

Recommendation 32 (statistics)

136. Section 27 of the new AML/CFT Act authorises the FIU to keep statistics covering, inter alia, the value of seized or confiscated property, and to publish a summary review of that statistical data in an annual report. The same section also authorises it, for the purposes of keeping statistics, to require public authorities to supply all necessary documents and information to the FIU. The statistics kept by the FIU include the number of cases disseminated to LEA and statistical data on the number of person prosecuted and convicted for money laundering and terrorist financing cases and the value of seized, confiscated and forfeited property for all offences and specifically for money laundering and terrorist financing. On the national level, data related to all criminal proceeds are kept also by Ministry of Interior – Unit of Information systems incorporated in Presidium of

Police Force. The Ministry of Justice should keep statistical data related to confiscation of property, as well as to the number of cases of confiscated and seized property. According to Slovak authorities, the statistics regarding the value of this property have been kept only since 1 January 2011, and the data on the first half of 2011 will be available in September 2011. In this context, it is relevant to reiterate the serious concerns raised above regarding the lack of coherence between different sets of statistics provided by various Slovak authorities.

137. Slovak authorities provided the evaluators with the following table that is related only to ML cases;

Table 11

	2005	2006	2007	2008	2009	2010	Total
Criminal prosecution	71	49	47	54	78	71	369
Prosecuted persons	57	25	28	22	39	25	195
Persons charged with a crime	19	5	19	7	12	10	72
Freezing measures[1]/value of frozen financial means in Euros	1/1.161.000	1/AB	1/416.978,22	1/5.000	1/5.000 1/10.000 13/70.244,55 1/13.000 1/3.000 1/875.035	1/3.761,47 1/234.308,49	11/ 2.797.32 7.73
Confiscation decisions[2]/value of confiscated financial means in Euros	1/VND		1/VND 1/30.000		1/T 1/T 1/electronics	2/T 1/C	9
Protective measures[3]					1/5xC 2/C	1/34.290,55 1/C	5
Number of measures – other method of freezing/seizure of a thing for the purposes of criminal proceedings[4]	C -14 T -5x M - 3000 €	C – 25 M : - 763.730,-SK, - 21.685-€, - 5.000-CZK, -10.000,-USD Other things -1	C -17 Other things - 1	C – 29 M - 5100 €	C – 67 Ship engine – 10x Construction engineering – 2x groceries - 1/26.000 € electronics and cars – 1/145.063,92€ Construction engineering	C – 42	

[1] – Section 95, Code of Criminal Procedure
[2] - Section 58, 60 Criminal Code
[3] - Section 83 s., Criminal Code
[4] - Section 89, 92,93, Code of Criminal Procedure – things handed over voluntarily for the purposes of criminal proceedings or things secured pursuant to separate laws (e.g. Act on Police Forces) – rendered back to the owner after criminal proceedings

(C- cars and motorcycles, T- Tobacco and cigarettes, M – Money, AB – Account Balance, VND-the value of things can not be determined)

Effectiveness and efficiency

138. From the statistics with regard to freezing and confiscation on ML cases, it seems that the implementation of this recommendation is ineffective. The amounts of confiscation for the years 2005 to 2010 are very low and demonstrate that confiscation is not used as a central tool for combating money laundering and predicate offences.

139. In addition, figures show that there were only 9 cases of confiscation during this period: 1 in 2005 (in which the value of the thing could not be determined), no confiscations in 2006, 2

confiscations in 2007 (the value of the first could not be determined and the value of the second amounting to 30,000 Euro), no confiscations in 2008, 3 confiscations in 2009 (for which no value was specified), and 3 confiscations in 2010 (for which no value was specified). These figures show clearly that the confiscation regime does not work effectively.

140. Moreover, no statistics have been made available as to the confiscation of proceeds of predicate offences, which also makes the assessment of the overall confiscation regime impossible.

141. More importantly, in the absence of any meaningful statistical information on freezing and confiscation, the Slovak Republic has not demonstrated that the implementation of this Recommendation is effective. The evaluators were frequently advised of the ease with which such measures could be frustrated through transfer of property to third parties. Thus this deficiency, identified in the 3rd round, has still not been addressed, and exacerbates the difficulty to effectively confiscate property

2.3.2 Recommendations and comments

142. Overall, though Slovakia has taken some legislative steps to comply with R.3, further legislative steps in order to fully comply with international standards appear to be needed. In addition, effectiveness of the implementation of seizure/freezing measures and forfeiture/confiscation should be improved as a matter of priority.

143. Precise statistics on amounts frozen, seized, forfeited and confiscated related to ML, TF and criminal proceeds should be maintained so as to be able to establish an overview of the effectiveness of the system.

144. Authority should be given to allow for confiscation from third parties and to prevent or void actions, where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in the ability to recover property subject to confiscation.

2.3.3 Compliance with Recommendation 3

	Rating	Summary of factors underlying rating
R.3	**PC**	• Confiscation of indirect proceeds for ML offences is unclear. • Though the confiscation from third parties is clearly provided by the law, the relevant provisions are not used in a sufficient manner in practice. • There are not sufficient provisions for protection of the rights of bona fide third parties. • There is no clear authority to take steps to prevent or void actions, whether contractual or otherwise, where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to confiscation. • Serious concerns over effectiveness of implementation.

2.4 Freezing of Funds Used for Terrorist Financing (SR.III)

2.4.1 Description and analysis

Special Recommendation III (rated PC in the 3rd round MER)

145. As a member of the EU, Slovakia freezes funds and assets of terrorists on the basis of EC Regulations and complementary domestic legislation. UNSCRs 1267 (1999), 1390 (2002), and 1455 (2003) are implemented by Council Regulation No. 881/2002[5] of 27 May 2002, whereas, the most important part of S/RES 1373/2001, is implemented by Council Regulation No. 2580/2001 of 27 December 2001. The Council Regulations once they are published in the Official Journal of the EU are directly applicable and binding law in Slovakia.

146. Separate sanctions regimes are applicable for non-EU-based entities or non-EU residents or citizens listed as terrorists (EU-externals) and for so called EU-internals. EU-internals are not covered by Council Regulation No. 2580/2001 due to the scope of the EU Common Foreign and Security Policy. Thus the EU adopted two Council Common Positions, No. 2001/930/CFSP and No. 2001/931/CFSP on the fight against terrorism, which are also applicable to persons, groups and entities based or resident within the EU (EU-internals), but their implementation, required subsequent enactment of national legislation.

147. In the meantime, although the half-yearly re-examination of the EU list as set out in article 1.6 of Common Position 2001/931/CFSP relates to all the names listed (listed persons and entities defined as "internal" and listed persons and entities defined as "external"), so far this has led only to the adoption of a new list for so-called "external" terrorists (Common Position 2009/1004/CFSP of 22 December 2009), with Common Position 2009/468/CFSP of 15 June 2009 remaining in effect for "internal" EU terrorists.

148. While Slovakia is relying on the abovementioned EU Regulations, given the shortcomings that have been identified in current EU procedures against EU-internals, a requirement to freeze assets of so-called EU-internals was adopted at the level of national legislation. Government Regulation No. 397/2005 Coll. (on execution of international sanctions to ensure international peace and security) contains the Government's list of sanctioned persons whose activity is confined to the territory of EU Member States or EU nationals. Financial institutions are obliged to freeze immediately all funds and economic assets of the persons included on the list in the Annex to Government Regulation No. 397/2005 Coll. This order has been updated 5 times (twice in 2006, once in 2007, 2008 and 2009 respectively) since it was enacted, most recently by Regulation 442/2009 in October 2009. This latest amendment bases itself on Common Position 2009/468/CFSP. There is no indication that the regulation has been updated to reflect subsequent changes in the EU sanctions list. In addition, the interlocutors from the Ministry of Finance who were in contact with the evaluators were not aware of any of the updates to the regulation, and in fact only provided the evaluators with the original regulation from 2005. The evaluators were not made aware of the subsequent updates until just before the pre-meeting that took place in May 2011. This fact gives rise to concerns over the effectiveness and applicability of the Government Regulation in practice.

[5] The last amendments to EC Regulation No 881/2002 imposing certain specific restrictive measures directed against certain persons and entities associated with Usama bin Laden, the Al-Qaida network and the Taliban were made on 16 March 2011 by approving EC Regulation No 260/2011.

149. Section 10 of Act 460/2002 provides the Slovak authorities with power to issue administrative penalties against natural and legal persons for violation of any international sanctions issued by the UN Security Council or by the EU Council. Under Section 3, as amended by the Act of 2005, the Government must announce the decision to impose sanctions "unless the Council has taken it over by common position or single action". However, the penalties of Section 10 can be based on violation of the international sanctions, without reference to any implementing measures on the part of the Slovak authorities.

150. The evaluators were informed during the on-site visit that draft legislation was in the process of preparation, though the text was not made available to the team. Therefore, the evaluators could not address this piece of proposed legislation in this evaluation.

Freezing assets under S/Res/1267 (c.III.1) and under S/Res/1373 (c.III.2)

151. The Slovak regime generally relies on the EC Regulations; therefore, certain shortcomings existing in the EU freezing system are valid in Slovakia.

.

152. As soon as the Sanctions Committee has made a designation, this must be followed by an amendment of the list of natural and legal persons listed in the annex to the Community Regulation. Freezing pursuant to Resolution 1267 must take place without delay.

153. As noted in other FATF or MONEYVAL evaluation reports, EU Regulations (only those adding names to the list of Regulation (EU) 881/2002 were reviewed in this context) in general are adopted quite some time after the decisions of the UN Sanctions Committee. Thus for the year 2009, for example, EU Regulations 344/2009, 490/2009, 574/2009 and 601/2009, of 24 April, 10 June, 30 June and 9 July 2009 respectively, add names to the list of designated persons and entities, while the decisions of the Sanctions Committee were dated 4 February, 27 May, 18 June and 29 June 2009 respectively, meaning that there were delays of between 10 days and more than two months. It would appear difficult to make this time any shorter (due in particular to considerations of consultation between departments and the time required for translation into all the official languages of the Union).

154. In the light of the above, it therefore appears that freezing measures cannot be deemed to having been taken without delay. Criterion C.III.1 is not fully met.

155. Insofar as Slovakia is concerned, Act 460/2002 does not require an additional announcement for sanctions decided by the EC in a Common Position or single action, so there should theoretically be no additional delay once the EU list has been updated. Regarding EU-internals, according to the Slovak authorities, the EU Regulations are supplemented by the Government Regulation 442/2009, which includes a provision requiring an immediate freeze of funds and economic assets of the persons included on the list in the Annex to the regulation. However, given that this Regulation and its accompanying annex have not been updated since 2009, as well as the fact that the representatives of Ministry of Finance, which is the responsible authority for the preparation of draft amendments to this Regulation were not aware of any updates made since 2005, serious effectiveness concerns are raised, particularly for persons who have been added to the EU lists or de-listed since that time.

156. According to the Slovak authorities, funds are generally frozen either in the course of a criminal proceeding (Section 95 of the CCP) or under Section 16 of the AML/CFT Act, which provides for suspension of any unusual business transaction (Article 4(2j) of the AML/CFT Act defines any act that may be linked to violations of international sanctions as unusual). Section 95 of the CCP refers generally to financial assets dedicated to committing a criminal offence, and not specifically to terrorism financing or international sanctions, but since violation of sanctions and

terror financing are both offences, it may cover these cases. It should be noted that Section 95 of the CCP allows a prosecutor to freeze funds before commencement of criminal proceedings, subject to judicial approval within 48 hours. This would seem to allow freezing without delay and without notification of the suspected party. However, the availability of Section 95 of the CCP depends on a link to a criminal investigation and prosecution. In addition, the effectiveness of these measures in practice cannot be assessed, in light of the fact that there has yet to be a case in which terrorist assets have been frozen by the Slovak Republic.

Freezing actions taken by other countries (c.III.3)

157. The Slovak authorities report that the freezing requests of other jurisdictions are handled at the EU level within the ordinary EU procedure, and if the EU lists a person requested by another jurisdiction and amends the lists prepared in accordance with Council Regulations 2580/2001, then obliged entities and Slovak authorities act accordingly to freeze that listed person's assets. An EU Member State or a non-member states has the possibility of presenting the Council with a listing request, this will be examined in the light of requirements of Common Position 2002/931 and the aforementioned Regulations; to be accepted it, must be the subject of a consensus decision by member states.

158. As far as the national level is concerned Government Regulation 397/2005 does not apply beyond the EU designations, since it does not refer to designations by countries outside the EU. Therefore, the evaluators conclude that Slovakia does not have any effective national law or procedure, apart from the EU's mechanism, to examine and give effect to the actions initiated under the freezing mechanisms of other jurisdictions, which ensure the prompt determination and the subsequent freezing of funds or other assets without delay.

Extension of c.III.3 to funds or assets controlled by designated persons (c.III.4)

159. The assets subject to freezing are defined by the EU Regulations are mostly line with c.III.4. However, the situation envisaged by the UNSCR 1267 for the freezing of assets in the event of control or possession of assets by persons acting in the name of or at the direction of designated persons or entities is not covered in Council Regulation No. 881/2002.

Communication to the financial sector (c.III.5)

160. The Slovak legal regime does not have any system for communicating actions taken under the freezing mechanisms referred to in c.III.1 - III.3 to the financial sector immediately upon taking such actions. For example, there is no procedure of notification of the financial sector of designations and instructions of, *inter alia*, freezing assets. The evaluators received the impression that, excluding EU-internals, banks are instructed to refer to the EU website, and no further communications are made by the Slovak authorities. However, banks seem to deal with the matter adequately, but this is a result of group policy rather than any official outreach policy of the Slovak authorities.

Guidance to financial institutions and other persons or entities (c. III.6)

161. Regarding the guidance to financial institutions and other persons or entities, the NBS in Section G of its "Methodological guidance…" No 4/2009 does address this issue. But this Guidance is only addressed to the banking sector. Indeed the awareness in the banking sector of obligations under international legal instruments to freeze any financial means is high. As was mentioned previously it is mostly due to the fact, that banks in Slovakia are mostly owned by large foreign financial groups, which implemented the said mechanism and have a group approach to compliance issues.

162. The Slovak authorities presented to the evaluators a notice sent to the banking sector on 4 April 2005 regarding the responsibilities of financial institutions relating to Council Regulation No. 881/2002 (relating to UN Resolution 1267), but the document was sent only to the banking sector and does not include operative instructions for a case in which a designated entity is identified.

163. From discussions held with the financial institution representatives, the evaluators did not receive any indication that guidance was sent to other financial institutions that may be holding targeted funds or other assets, concerning their obligations in taking actions under freezing mechanisms.

164. It is also important to note that there are no guidance notes whatsoever issued to DNFBP, and the level of awareness in this sector may be described as less then adequate. The evaluators were also not made aware of any day-to-day consultations with this sector on the matter in hand.

De-listing requests and unfreezing funds of de-listed persons (c.III.7)

165. Relevant EU Regulations do not provide for a national autonomous decision for considering de-listing requests and unfreezing as a whole. As such any freezing remains in effect until otherwise decided by the EU. Common Position 2001/931/CFSP of the European Union implements S/RES 1373 (2001) and provides for a regular review of the sanctions list which it has established. Moreover, listed individuals and entities are informed about the listing, its reasons and legal consequences. If the EU maintains the person or entity on its list, the latter can lodge an appeal before the General Court in order to contest the listing decision. De-listing from the EC Regulations may only be pursued before the EU courts.

166. However to ensure such a procedural fairness, Slovakia should have a publicly available procedure in place for any individual or entity to apply for a review of the designation from the designating authority, with the ability to seek further review of an adverse finding by the designating authority, to a review body. Slovak authorities were not able to advise the evaluators about the existence of any effective and publicly-known procedures for considering de-listing requests and for unfreezing the funds or other assets of de-listed persons or entities in a timely manner consistent with international obligations. As at the time of the on-site visit, there had not been any cases in Slovakia requesting de-listing.

167. The evaluators did receive the impression that there was no Slovak authority responsible for advising individuals as to the procedures necessary for requesting de-listing or related matters. Furthermore, there is no procedure for de-listing requests and for unfreezing the funds or other assets of de-listed persons with regard to EU-internals, according to Act No. 397/2005. In light of the above, it was not clear to the evaluators that there are procedures or guidance at the disposal of a Slovak resident or citizen who finds himself erroneously listed or Slovak authority to which such an individual could refer. Therefore, essential criterion c.III.7 is not met.

Unfreezing procedures of funds of persons inadvertently affected by freezing mechanisms (c.III.8)

168. The Slovak authorities refer to European Council Regulation 2580/2001, Article 6, which allows the competent authorities of a Member State to grant specific authorisations to unfreeze funds, other financial assets or other economic resources. The competent authorities listed in the EC Regulation No 2580/2001 are the Ministry of Finance and the Ministry of Interior.

169. The Slovak authorities argue that in practice unfreezing procedures shall be initiated by a person wishing to unfreeze his/her frozen funds through the court. On the basis of successful

handling of the matter at the court, Slovak authorities understand that the decision of the court shall further be delivered to the Commission to deal with the matter at the EU level.

170. There is no specific procedure which deals with unfreezing in a timely manner the funds or other assets of persons or entities inadvertently affected by a freezing mechanism upon verification that the person or entity is not a designated person. Reference to the court is naturally always a possibility and is not sufficient to meet this requirement. Furthermore, the authority granted in section 6 of Regulation 2580/2001 requires consultation with other Member States, the Council, and the Commission. Therefore, it does not seem possible for a national court to fill this role. If so, it is not clear to the evaluators that there is a Slovak authority competent to unfreeze assets and perform other actions under Section 6 of Regulation 2580/2001 when necessary. Consequently, the de-listing procedures cannot be considered "publicly known" as required by c.III.8. However, with regards to declarations against EU-internals made in accordance with the Slovak regulations, persons or entities whose assets have been frozen under the national measure pursuant to Act No. 460/2002 Coll. can challenge the measure in the first instance at the body who first issued the decision, pursuant to no. 71/1967 Coll. Administrative Procedure Code. If he or she is not satisfied with that body's decision, he or she may challenge it at the competent civil court pursuant to Sections 246 and 246a of the CCP (Act no. 99/1963 Coll., Fifth Part, Sections 244 – 250s). The appropriate court varies depending on whether the freezing decision has become final or not. It would seem that in this case, the unfreezing process is clear and publicly known.

Access to frozen funds for expenses and other purposes (c.III.9)

171. Regarding persons and entities linked to Osama bin Laden, the Al-Qaeda network and the Taliban pursuant to S/RES/1267(1999), Regulation (EC) No. 881/2002 of 27 May 2002, as modified by Council Regulation (EC) No. 561/2003 of 27 March 2003, includes Article 2b relating to unfreezing sums for the purposes of covering expenditure of a humanitarian nature. The competent national authorities may unfreeze sums which are: (i) necessary for basic expenses, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums and public utility charges; (ii) intended exclusively for payment of reasonable professional fees and reimbursement of incurred expenses associated with the provision of legal services; (iii) intended exclusively for payment of fees or service charges for routine holding or maintenance of frozen funds or economic resources; or (iv) necessary for extraordinary expenses.

172. The Sanctions Committee must be notified of the decision, and in the case of use of funds established by virtue of points (i), (ii) or (iii), if the Sanctions Committee has not taken a decision to the contrary by the end of the mandatory period of three working days, or, in the case of use of funds on the grounds of point (iv), if the Sanctions Committee has approved this use, exemption is granted.

173. Any person wishing to benefit from these provisions must send their request to the relevant competent authority of the Member State listed in Annex II of the Regulation. The competent authority specified in Annex II must notify the person having presented the request in writing, as well as any other person, entity or body recognised as being directly concerned, if the request is granted. The competent authority also informs the other member states of whether or not the derogation has been granted. For Slovakia, the competent authorities are the Ministry of Finance and the Ministry of the Economy. Such measures have not been tested in Slovakia. Criterion III.9 is met.

Review of freezing decisions (c.III.10)

174. Persons and entities targeted by Regulation 881/2002 may appeal against the aforementioned Regulation under ordinary law provisions applicable to EU decisions, i.e. by referring the case to

the General Court. Similarly, persons targeted by Regulation (EC) No. 2580/2001 may appeal against the aforementioned regulation under the same procedures by referring the case to the same European Court. There are a number of cases before the General Court., and appeals against freezing orders based on Council Regulations (EC) No. 2580/2001 and 881/2002, that are pending in the General Court. In addition, as mentioned above, persons or entities whose assets have been frozen under the national measure can challenge the decision at the body who first issued the decision and at the competent civil court. Therefore criterion III.10 is met.

Freezing, seizing and confiscation in other circumstances (applying c.3.1-3.4 and 3.6 in R.3, c.III.11)

175. Slovak law relating to confiscation and seizure are of general application; consequently, the measures in place pursuant to Recommendation 3 apply to funds or other assets relating to terrorism other than those targeted by Resolutions 1267 and 1373. The loopholes identified in Recommendation 3 therefore concern freezing, seizure and confiscation of funds or other assets relating to terrorism outwit the application of Resolutions 1267 and 1373. In addition, certain deficiencies noted with regard to SR.II might also be relevant to this criterion, particularly those related to the definition of "funds" and the extent of the terrorist financing offence under article 419(b) of the SCC, as these might limit the ability to prosecute persons for terrorist financing and thus limit the ability to rely on the mechanisms provided in article 95 of the CCP. Criterion III.11 is not fully met.

Protection of rights of third parties (c.III.12)

176. As discussed above under Recommendation 3, section 45 of the CCP gives any party whose thing was seized the right to participate in the legal seizure proceedings. However, the limitations mentioned above regarding R.3 apply here as well.

Enforcing obligations under SR.III (c.III.13)

177. The 3rd round MER noted that no appropriate measures to monitor effective compliance under SR III were in place. The evaluators received the impression that, other than periodical written updates from banking institutions in accordance with Section 91(8) of the Act on Banks No. 483/2001 Coll., the appropriateness of which is questionable, there has been no improvement achieved in the Slovak system in this regard; particularly in relation to other financial institutions and DNFBPs. The evaluators believe that this is a result, *inter alia*¸ of the fact that there is no person or body that sees itself as responsible for these obligations.

178. As noted in the 3rd round MER, the legal mechanism for sanctioning breaches of the relevant legislation exists in Slovak legislation, however, it has never been used. The Slovak authorities did not provide any further information regarding such sanctions imposed in practice. Therefore, the deficiencies noted in the 3rd round MER continue to pertain.

Additional element – Implementation of measures in Best Practices Paper for SR.III (c.III.14) & Implementation of procedures to access frozen funds (c.III.15)

179. The Slovak authorities again rely on the EU regulations regarding these issues. But not all of the measures set out in the Best Practice Paper have been implemented.

180. Articles 5 and 6 of Council Regulation (EC) No. 2580/2001 provide for exemptions comparable to those provided in Council Regulation (EC) No. 881/2002 as amended. They provide for the possibility to authorise the access to funds or financial assets of economic resources, if they have been determined to be necessary for the purposes set forth in Section 1(a) of the S/RES 1452 (2002). The procedure to be followed is comparable to the one for exemptions under Council

Regulation (EC) No. 881/2002. However, no notification of the Sanctions Committee is foreseen. Instead, prior notification of other member states of the EU is mandatory in some cases. Comparable exceptions are also available in Section 9 of the Act No. No.460/2002 Coll. on execution of international sanctions providing the international freedom and security as amended by the Act no. 127/2005.

Recommendation 32 (terrorist financing freezing data)

181. Slovak authorities reported only one case where a bank refused to perform an attempted transfer of €10,200 from a personal account to an account of a listed person. In this case the reason for the transfer was stated as "payment for the goods". Because of the matches with the UN Consolidated list of individuals and entities subject to the assets freezing, this operation was refused by the bank. Apart from this case, no funds have been frozen in accordance with the UN or EU Regulations

Effectiveness and efficiency

182. According to the Slovak authorities, there has not yet been a case of freezing of assets under the UNSCRs. This fact gives rise to concerns over the effectiveness of the existing procedures.

2.4.2 Recommendations and comments

183. The Slovak Republic needs to develop guidance and communication mechanisms with all financial institutions and DNFBPs and a clear and publicly known procedure for de-listing and unfreezing in appropriate cases in a timely manner.

184. Currently, except for the periodic reports from banking institutions, there does not seem to be any monitoring or compliance regarding these obligations. A more robust and effective mechanism, beyond the periodic those reports submitted by the banking sector, for the monitoring of the compliance of reporting entities with the SR III requirements should be established.

185. The evaluators were informed that draft legislation was in the process of preparation, though the text was not made available to the team. Therefore, the evaluators could not address this piece of legislation. It is of great importance that the Slovak authorities utilise this opportunity to bring themselves fully into compliance with SR.III.

2.4.3 Compliance with Special Recommendation SR.III

	Rating	Summary of factors underlying rating
SR.III	**PC**	• The situation envisaged by the UNSCR 1267 for the freezing of assets in the event of control or possession of assets by persons acting in the name of or at the direction of designated persons or entities is not covered in Council Regulation No. 881/2002. • The time taken for EU Regulations to be adopted aimed at dealing with amendments made to the list published by the 1267 Committee can be relatively long; in this respect the obligation to freeze terrorist funds without delay is not observed. • 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. • Insufficient monitoring for compliance of financial institutions and DNFBPs.

Authorities

2.5 The Financial Intelligence Unit and its functions (R.26)

2.5.1 Description and analysis

Recommendation 26 (rated PC in the 3rd round MER)

Legal framework

186. Recommendation 26 was rated "*Partially Compliant*" in the 3rd round MER. The main deficiencies identified were the lack of explicit reporting obligation on TF suspicion, the absence of guidelines or indicators issued to the financial sector on "unusual business activity", an unclear reporting system and the lack of any publications to the financial sector or otherwise covering statistics, typologies and trends in the AML/CFT field. The report also noted the concerns over the operational independence and autonomy of the FIU which were arising from the identified weak position of the FIU in the existing police structure.

187. The Slovak Financial Intelligence Unit (FIU) was established on 1 November 1996 within the Slovak police as a law enforcement style FIU. As of 1 January 2004 the FIU became one of the 8 divisions in the Bureau of Organised Crime, under the first Vice President of Slovak Police. At the time of the 3rd round evaluation, there was no separate legal act defining the roles and responsibilities of the FIU.

188. The major legal change since 3rd round evaluation has been the introduction of the new AML/CFT Act, which came into force on 1 September 2008. The 6th Part of the AML/CFT Act prescribes in details all competencies and responsibilities of the Slovak FIU.

Establishment of an FIU as national centre (c.26.1)

189. Pursuant to subsection (1) of Section 26 of the AML/CFT Act, the FIU shall serve as a national unit for the area of the prevention and detection of legalisation and terrorist financing. It shall receive, analyse, evaluate and process unusual transaction reports (hereinafter referred to UTRs) and other information related to legalisation of proceeds or terrorist financing for fulfilling the tasks under this Act or under Section 2 of the Act on Police Force. According to Section 2 of the Act on Police Force, the police force performs the following tasks: "…b) detect criminal acts and identify their perpetrators, c) co-operate in detection of tax evasions, illicit financial transactions and legalisation of incomes from criminal activities and financing of terrorism…"

190. While its roles and responsibilities are clearly stated in laws, the FIU itself was not established by law or regulation. The FIU was established by the Personal Order of the Minister of Interior of the Slovak Republic No. 483/1996 based on the Resolution of the Government of the Slovak

Republic No. 206/1996. This competence of the Minister of Interior is based on Article 4 of the Act on Police Force that authorises the Minister of Interior to establish and abolish services of the Police Force, which operate within the divisions of the Police Force. The appointment of the head of the FIU and the FIU's organisational structure were both established by a decision of the Head of the Bureau for Combating Organised Crime No. 52/2009 on Organisational Order of the Bureau for Combating Organised Crime. It is concluded that the Slovak FIU, having been incorporated into the Bureau for Combating Organised Crime, serves as a national centre for receiving, analysing and disseminating disclosures of UTR and other information in relation to suspected ML and TF activities

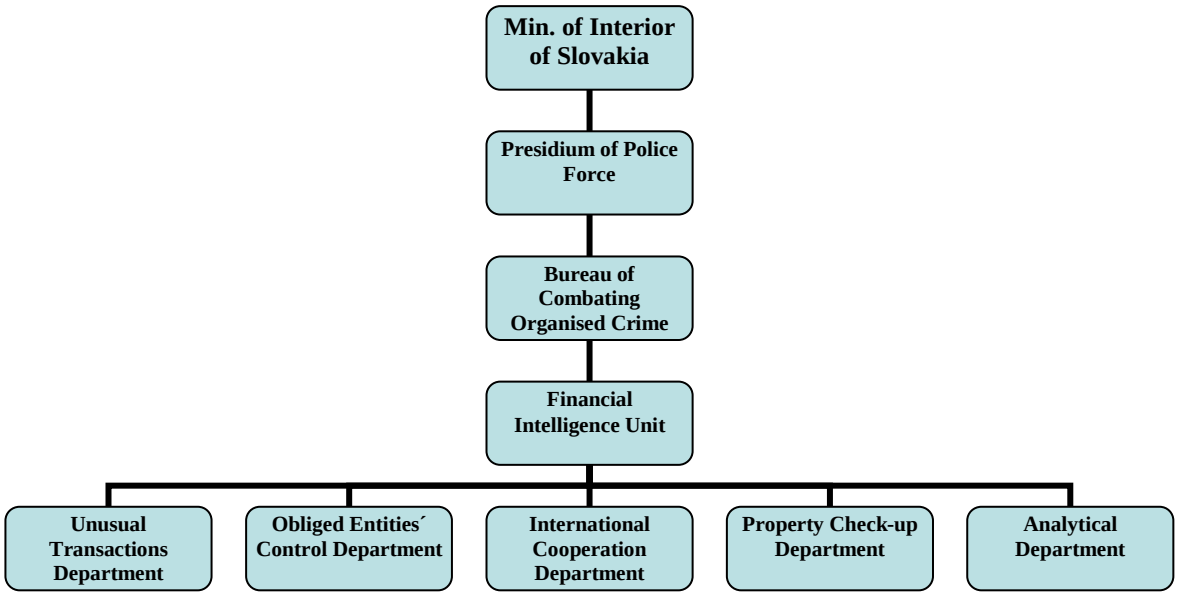
191. Section 23 Order of the Head of the Bureau of Combating Organised Crime of Presidium of Police Force No. 52/2009 on Organisational Order of the Bureau of Combating Organised Crime of Presidium of Police Force states:

"Financial Intelligence Unit

(1) Financial Intelligence Unit has its seat in Bratislava.
(2) Financial Intelligence Unit is divided as follows:
- *a) unusual transactions´ department,*
- *b) obliged entities´ control department,*
- *c) international co-operation department,*
- *d) property check-up department,*
- *e) analytical department.*

(3) Financial Intelligence Unit shall especially:
- *a) map, detect and destruct organised groups in the field of tax criminal activity, money laundering, unlawful financial operations, capital and financial market and terrorist financing,*
- *b) perform operational-search activity aimed at operational detection of particularly serious criminal activity, especially tax criminal activity, money laundering, unlawful financial operations, capital and financial market and terrorist financing and build up network of informers and receive other information sources,*
- *c) in scope of its competence ensure co-operation with units of the Bureau and law enforcement bodies in search of and documenting criminal activity, gather, evaluate and make use of especially financial and economic information important for combating money laundering and take measures,*
- *d) perform tasks resulting from a special regulation 1),*
- *e) methodologically manage and in selected cases co-ordinate the activity of financial police departments of units Bratislava, West, Central and East of the Bureau, decide about dissemination of information obtained by Financial Intelligence Unit upon the performance of reporting obligation under a special regulation 1) to a unit of the Bureau with local competence for verification,*
- *f) in scope of its competence ensure co-operation with relevant domestic and international authorities, organisations and institutions."*

192. The Slovak FIU currently consists of the following departments: The Unusual Transactions Department, the Obliged Entities Control Department, the International Cooperation Department, the Property Check-Up Department (Asset Recovery Office) and the Analytical Department.



193. The Unusual Transactions Department mainly deals with UTRs. It receives, analyses, evaluates and processes UTRs. Besides processing of received UTRs it is authorised to give advice and guidance to obliged entities on how to recognise unusual transactions and on specific indicators linked to possible ML or TF cases. As advised by the authorities, this form of providing guidance and feedback is performed on a daily basis. In case that the facts indicate that a criminal offence was committed it submits a case to the law enforcement authority (police investigator) or to the tax authority if the information is relevant to commence tax proceeding.

194. In turn, the main task of the Analytical Department is to collect, keep and analyse statistical data on ML and TF at the national level. It is responsible for the provision of feedback to reporting entities on the efficiency of UTRs received by the FIU. The Analytical Department prepares and publishes the annual report of the Slovak FIU as well. In addition, it supports the analysis of unusual transactions in complex and serious cases where more transactions and money flows are involved. Employees of this department are in charge of making schemes using analytical IT product of i2's Analyst's Notebook.

195. Police officers of the Check-up Property Department trace, gather and make use of financial information considerable for identification of crime proceeds. They closely co-operate with the Unusual Transactions Department in cases where it was found out that there is a suspicion of commission of crime. They make an "asset profile" on concrete person and together with other financial information from unusual transaction report. This comprehensive intelligence package is then submitted to the law enforcement authority for further action.

196. One very important power of the FIU is the authority to postpone the execution of suspicious transactions. Section 16 of the AML/CFT Act prescribes that the FIU can order postponement of a transaction for a maximum of 48 hours and if the case is transferred to law enforcement authorities, for an additional 24 hours. Reporting entities are obliged to postpone transactions themselves if there is a danger that the execution of the transaction may hamper the future seizure of funds.

197. In 2009, the FIU used this authority in 69 cases in a total amount of EUR11,508,280. Out of these numbers, prosecutor's office seized €2,211,260 in 14 cases. Criminal offences reported in these cases were fraud, tax and insurance evasion, sharing, establishing, and contriving and supporting a criminal group. In the first half of 2010, 41 transactions have been postponed in a

total amount of €1,894,394, which resulted in 4 seizures by the prosecutors in total amount of €33,114. (The same offences were reported as underlying offences).

Guidance to financial institutions and other reporting parties on reporting STRs (c.26.2)

198. Section 17 (2) and (3) of the AML/CFT Act itself provides for possible manners of reporting UTRs and the information that has to be included in a UTR in detail.

199. In addition, the NBS issued in collaboration with the Ministry of Finance and the FIU the "Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing". This Methodological guidance deals with overall systems that banks should put in place, with one section dealing with the detection and reporting of unusual transactions. It should however be noted that this Guidance address only to banks.

200. In addition to the guidance given to the banking sector through the mentioned Methodological guidance, the FIU has published "Guidelines for obliged entities related to observance of obligations stipulated in Section 14 of AML/CFT Law in connection with detection of unusual transaction ("UT")" on its web site. These guidelines are addressed to all reporting entities and provide for brief elaboration of the steps that reporting entities should undertake in order to effectively detect unusual transactions. Another piece of guidance to reporting entities, which was provided by the FIU on its web site, is "Advice to reporting entities related to deficiencies in content of reports on unusual transactions". This document aims at drawing the attention of reporting entities to repeated deficiencies in reports that are spotted by the FIU.

201. Reporting forms for banks, insurance, real estate agencies, as well as one general form for other obliged entities are published on the web site (http://www.minv.sk/?vzory) of the Ministry of Interior. The evaluators noted that reporting entities from the financial sector are very well aware of the existence of the said forms. It appeared that they use these forms, although some of the interviewed entities stated that the present form is not very user friendly and that it could be less time consuming. The evaluation team was advised that the forms were agreed in the meetings between the FIU and the sectors' representatives while their content is strictly based on the provisions of the AML/CFT Act.

202. A certificate for using the protected system of electronic reporting is issued to every reporting entity which reported more than twice. The evaluators noted that the UTRs are received on a computer which is isolated from the rest of the IT system. Once received, the report is entered into the database of the FIU. Every report received results in a case opened by the FIU, which is reflected in the statistics in Annex XIX. This report is checked in the FIU databases, police databases, and publicly available sources. Each time the account statements of persons involved the case are collected as well. After completion of the data collection process, the whole case is analysed in order to confirm or eliminate primary suspicion.

Access to information on timely basis by the FIU (c.26.3)

203. The authorities indicated that the FIU has direct access to the following law enforcement databases:

- Information systems of Ministry of Interior of the Slovak Republic and the Police Force: centralised information system "Centrálna lustračná konzola" and also particular isolated information systems such as:

- Register of population (identification of a person, birth identification number, date of birth, address of stay, family members, identification documents including passports, wanted persons),
- Register of vehicles, information of traffic administration agenda, information on restricted vehicle license numbers, information on registration of arms, ammunition and firing ranges, wanted arms, information on registration of foreigners with stay permits in the territory of the Slovak Republic, information on undesirable persons,
- Register of persons in the interest of police (so-called „ZOP"), information on criminal activities of a person (so-called "OTE"),
- Information on the current state of criminal prosecution against perpetrators within Police Force (so-called „AVÍZO"),
- Information of the service of border police for the purpose of control of persons and vehicles,
- Information on wanted persons, identification of found corpses, information on stolen vehicles, stolen or lost vehicle license numbers,
- Centralised register of seized, released and found vehicles, identified and returned vehicles,
- System of dactyloscopic identification of persons,
- Complete register of firm lines and cell phone numbers,
- Centralised register of prisoners,
- Centralised register of prison service in the Czech Republic,
- Register of criminal prosecution files (so-called „DVS").

All these databases, with the exception of the centralised register of prisoners and the centralised register of prison service in the Czech Republic that are held by the Ministry of Justice, are held by the Ministry of Interior.

204. The following information can be obtained directly from open sources:

- Land Registry – search based on the birth identification number of a person or the registration number of a company via privileged password access that is given to the FIU based on the agreement with the Land Registry. General public cannot search database according to these parameters. Following data is at disposal of the FIU analytical staff:
  - *parcels* - parcel number, land area, type of parcel, way of use of parcel, location of parcel, legal relationship;
  - *buildings* – registered number, type of building, description of building, location of building;
  - *owners* – surname, name, date of birth, birth identification number, address or name of legal entity, registration number, seat, share of co-owners;
  - *land charges*.

- Business Registry of the Slovak Republic and Small Business Registry of the Slovak Republic - Following information on legal and natural persons can be obtained directly from these sources:
  - Business name;
  - Registered seat;
  - Registration Number;
  - Date of entry into Business Registry;
  - Legal form;
  - Scope of business;
  - Partners/owners;
  - Amount of investment;
  - Statutory pointy (proxies);
  - Capital.

205. The FIU has indirect access to the following information upon written request:

- information and additional documents from state authorities, villages, legal and natural persons under paragraph 1 of Section 76 of the Act No. 171/1993 Coll. on Police Force as amended, (See Annex X) According to this section state authorities, municipalities, legal and natural persons are obliged to provide requested documents and information without delay if reasons stipulated by other general binding legal regulations do not prevent them to do so. Practical experience shows that requests are responded within 30 days at the latest following delivery of the request, as advised by the authorities. Provision of Section 76 is used for performing all FIU functions including classical FIU functions.

- Information related to clients of banks or foreign bank branches under paragraph 4 of Section 29a of the same Act, although falling under the bank secrecy (under paragraph 4 of Section 91 of the Act No. 483/2001 Coll. on Banks and on amendments and supplements to certain legal acts as amended), when detecting tax evasions or unlawful financial operations or legalisation of proceeds of criminal activity and thereto related criminal offences and their perpetrators.

206. It seems that the FIU has direct or indirect access to a vast number of different databases, which serves as a solid basis for its analytical work. Evaluators consider this access as being "on a timely basis" as required by international standards, especially bearing in mind the considerable volume of data which is accessed directly. Furthermore, all databases are integrated within a satisfactory IT system which is constantly being improved. This enables the FIU to act quickly and effectively in its analytical functions.

207. The FIU also maintains its own database of received UTRs.

Additional information from reporting parties (c.26.4)

208. Pursuant to paragraph 5 of Section 17 of the AML/CFT Act obliged entities are required to notify additional information to the unusual transaction report and provide thereto-related documentation on the unusual transaction to the FIU on the basis of a written request. Authorities advised to the evaluators that additional information requested is provided without undue delay. The FIU states in a request the timeframe in which the request should be executed. The usual time for a response is two to three days. Based on Section 17 (5) of the AML/CFT Act the FIU may request data only from the reporting entity which submitted the UTR. For any other additional information related to UTR the FIU may make use of provision of Section 21 of the AML/CFT Act, Section 29a (4) of the Act on Police Force and Section 76 (1) and (2) of the Act on Police Force.

209. In addition to the abovementioned competences for requesting data and information from reporting entities, the Slovak FIU is incorporated into the financial police, thus it is authorised to obtain information when detecting tax evasions or unlawful financial operations or legalisation of proceeds of criminal activity and thereto related criminal offences or terrorist financing and their perpetrators as it is stipulated by paragraph 1 of Section 29a of the Act No. 171/1993 Coll. on Police Force and also information related to clients of banks or foreign bank branches under paragraph 4 of Section 29a of the same act. All these competences set out in the Police Force Act can only be used by police officers of the services of the criminal and financial police. (Section 38a).As advised by the FIU, its employees participate in investigations together with investigators from other units only in urgent cases.

Dissemination of information (c.26.5)

210. Paragraph 2 (letters b and j) of Section 26 of the AML/CFT Act authorises the FIU to disseminate financial information to domestic authorities for investigation. According to this provision, the FIU shall:

b) submit a case to law enforcement authorities if the facts indicate that a criminal offence has been committed,

j) provide the tax administrator with information obtained by performing its reporting obligation provided that such information substantiates the commencement of tax proceedings or is essential for the ongoing tax proceedings unless the fulfilment of the FIU's tasks is endangered.

211. The evaluators have interpreted this provision that it authorises the FIU to disseminate information that might be related to any criminal offences including ML and TF offences having been committed. This interpretation was also confirmed by the authorities.

212. In addition, paragraph 3 of Section 26 of the AML/CFT Act requires the FIU to provide all information and documents obtained under the AML/CFT Act to the state authorities that perform tasks related to protection of constitutional order, internal order and state security. The FIU maintains, for these purposes, a separate database containing information extracted from every UTR received.

213. Statistics provided show a significant increase in the number of disseminations to law enforcement authorities from 17 in 2008 to 816 in 2009, as opposed to previous years. As advised by the authorities, this increase in statistics is a result of a new approach in maintaining it. Statistics in previous years reflected only cases disseminated according to the AML/CFT Act. However, statistics kept since 2009 reflect all disseminations done by the FIU in its implementation of the new AML/CFT Act in the next paragraph.

214. The 122 cases pursuant to Section 26 paragraph 2 letters (a) and (b) of the AML/CFT Act. According to letter (a any indication on any criminal offence is disseminated to law enforcement authorities for fulfilling the tasks of the police force defined in Article 2 of the Act on Police Force. According to letter (b) if the facts indicate that a (any) criminal offence has been committed they are disseminated to investigators in order to conduct criminal investigation. As advised by the authorities approximately 70% of the disseminated cases have been related to ML offences. During the on-site visit, the Evaluators were advised by the FIU that the statistics provided for the first half of the year 2010 (See Table below) have the following meaning: out of 415 disseminated cases in the mentioned period, 119 cases were disseminated according to Section 26 paragraph 2 letter (b) of the AML/CFT Law, while the rest of the cases were disseminated according to Section 26 paragraph 2 letter (a) for fulfilling the tasks of the Police Force defined in Article 2 of the Act on Police Force.

215. Approximately 70% of 119 cases disseminated in the first half of 2010 refer to ML offences, as advised by the FIU. This leads to the conclusion that around 80 cases on ML have been disseminated in the reference period. As advised by the authorities, the most of these predicate offences in the said period were related to tax offences, fraud, establishing, contriving and supporting a criminal group, sharing, unlawful manufacturing and use of electronic payment means and other payment card and trafficking in migrants. The figure of 415 disseminating cases in the first half of 2010 was presented to evaluators in the MEQ and was discussed in considerable details during the on-site visit. That figure has changed in the present report due to the fact that other sets of statistics have been provided to evaluators later on, during the course of evaluation process. The figures (415 disseminated cases, 119 disseminated according to the

AML/CFT Law, etc.) presented here are still needed as an indication that approximately 20% of cases disseminated by the FIU relate to ML cases.

216. Significant attention here is given also to providing information to tax authorities which reported that 442 UTR based cases were received from the FIU in 2009. 329 such cases were received in the period from 1 January to 22 September 2010. Tax authorities receive entire cases, not just extracts from UTRs. All these cases are transferred to local tax authorities for the purpose of collecting tax revenues. Information that could hamper possible criminal proceedings or performance of the tasks of the FIU (e.g. banking information, information obtained through the use of special investigation techniques) is extracted and not sent to tax authorities. If there is a suspicion of any criminal offence of tax evasion or tax fraud the case is referred to the law enforcement body that is authorised to initiate the criminal investigation. If there is information available to the FIU, which can be useful just for collection tax revenues, the case is referred to the tax authorities. In these cases the decision to which authority the case should be referred to is made by the head of the FIU.

Operational independence and autonomy (c.26.6)

217. The FIU is one of the departments of the Bureau for Combating Organised Crime of Presidium of Police Force. The Presidium of Police Force is in the Ministry of Interior.

218. The FIU is hierarchically subordinated to the Minister of Interior, the President of the Police Force and the Director of the Organised Crime Bureau. The Director of the FIU is appointed by decision of the Director of the Organised Crime Bureau. Turnover of directors is very high. At the time of the on-site visit, the new director had only been in the post for several months. The previous director held the position for three years, which is record a duration, as advised by authorities. The 3rd round MER also emphasises the fact that directors changed three times during the period of four years preceding the report.

219. Although the Slovak authorities are explicit in interpretation that the FIU has an adequate level of operational independence, which has been confirmed in practice, no legal safeguards have been introduced in this regard. However, evaluators have not heard any indication that the operational independence of the FIU has been breached so far.

220. The FIU does not have its own budget. Decisions on execution of the budget are taken at superior level. The FIU is authorised to propose the execution of the Police Force budget. As advised by the authorities, one part of that budget reserved for the FIU's activities, and that whenever substantial requirements of the FIU Slovakia were introduced to the Bureau of Combating Organised Crime they were fulfilled and financial sources for activities approved. There is no fixed term of office for the Head of the FIU. No formal grounds for dismissal of the Head of the FIU are introduced nor is the procedure for appealing the decision to dismiss. The Head of the FIU is a police officer. The nomination, appointment and suspension of police officers in relation with superior functions are defined by Article 33 of the Act No. 73/1998 Coll. on Civil Service of the Officers of the Police Force, Slovak Information Service, Penitentiary and Justice Guard Force and Railway Force as amended. These rules apply for all police officers and state that "Any police officer shall be appointed and suspended from his function by respective superior" (paragraph 2 of Section 33.).There is no fixed term of office for the Head of the FIU. No specific formal grounds for dismissal of the Head of the FIU are introduced. With regard to procedure for appealing the dismissal decision, there is a general procedure for appealing decisions stipulated by Act No. 73/1998 in its Sections 242 and 244 (see Annex IX), but there is no specific procedure for appealing decision to dismiss which would be applied against the formal grounds for dismissal.

221. Bearing in mind also other legal provisions which are explicit in giving the FIU a leading role in the whole system, it appears to the evaluators that it still has rather weak position in overall police structure. The 3rd round MER emphasised this issue but apart form defining its roles in laws nothing has been formally done to strengthen the position of the FIU.

Protection of information held by the FIU (c.26.7)

222. The evaluators had a chance to visit the FIU and witness how the information held by the FIU is protected.

223. In terms of technical security, the evaluators noted that all kinds of obtained information are saved in and stored in an internal autonomous FIU database. Each employee has direct access to this database on the basis of their own login and password access. It is possible to monitor and check all users who have accessed to the database.

224. As far as the building security is concerned, all premises of the FIU are connected to a centralised security desk and any security violation is signalised. The FIU premises are separated from the rest of the building of the Police Force Headquarters. Employees can enter the premises by entering a personal code.

225. The staff of the Slovak FIU is obliged to keep secrecy as stipulated in paragraph 4 of Section 18 of AML/CFT Act. This paragraph which reads as follows: *"Obligation of keeping secrecy shall be kept by any person who, in the course of performance of tasks of the Financial Intelligence Unit or in relation to them, becomes aware of information obtained under this Act."*

226. The evaluators believe that the information held by the FIU is protected securely and disseminated only in accordance with the law.

Publication of periodic reports (c.26.8)

227. Section 27 of the AML/CFT Act implicitly requires the FIU to release annual reports, which deals with keeping statistical data. According to this paragraph, the FIU shall keep summary statistical data covering the number of unusual transaction reports received, the particular ways of processing unusual transaction reports and their number including the number of cases submitted to law enforcement authorities or tax administrators for a calendar year as well as the number of persons prosecuted, the number of persons convicted of legalisation of proceeds from criminal activity and the value of seized property, confiscated property or forfeited property and once a year the FIU shall publish a summary review of that statistical data in an annual report. Reports of the FIU shall comprise information on its activities.

228. The Slovak FIU has issued its first annual report for the year 2009. It contains four chapters on the history of the FIU and its organisational structure, legal framework of the FIU and its functions, description of the FIU's activities in general and activities undertaken in 2009, statistical data related to ML offences, all criminal offences and cross-border cash declarations. No typologies and trends were presented in this report nor was this required by the Law. Nevertheless, some reports on typologies and trends in AML CFT area have been published on the FIU web site. Evaluators have been provided with "Guidelines for leasing companies" which describe some fraudulent actions related to interconnected companies, "Guidelines for credit institutions" related to misuse of EFT POS terminals, to tax criminal offences, to procedure upon the discovery of case of phishing and pharming, to false identification documents, and to potential way of terrorist

financing connected with one legal entity from United Arab Emirates. Also, "Guidelines for advocates related to misuse of client account" has been provided.[6]

Membership of Egmont Group & Egmont Principles of Exchange of Information among FIUs (c.26.9 & 26.10)

229. The Slovak FIU has been a member of the Egmont Group since June 1997.

230. The FIU respects all criteria and carries out its activities as it is stipulated by Egmont Group Statement of Purpose and its Principles for Information Exchange between FIUs. Within international co-operation by exchanging information related to ML and TF between FIUs via Egmont Group network or FIU.NET, the Slovak FIU has co-operated with more than 61 foreign FIUs from total number of its 115 counterparts united through Egmont Group network.

Recommendation 30 (FIU)

Adequacy of resources to FIU (c.30.1)

231. The FIU is a specialised unit of the Police Force of the Slovak Republic integrated in the structure of Presidium of Police Force as a division in the Bureau of Combating Organised Crime. The FIU consists of 5 departments:

- The Unusual Transactions Department,
- The Obliged Entities Control Department,
- The International Cooperation Department,
- The Property Check-up Department (Asset Recovery Office),
- The Analytical Department.

232. The staff of the FIU working for the above mentioned departments, including superiors, the Deputy Head and the Head of the FIU, are all police officers of the Police Force of the Slovak Republic. The required professional qualifications for their positions include a university degree, preferably in law, security services and economics, and previous practice within the police force.

233. The FIU employs 37 police officers and 1 civil servant as at the time of the on-site visit. In Unusual Transactions Department, which deals with analysis of unusual transaction reports, there are eight police officers including the head of department.

234. The premises of the FIU are situated in the Police Force Headquarters building, but are separated from the rest of the building. It seems that the space of these premises is adequate in for the present number of staff. Authorities informed the evaluators that the budget for the reconstruction of premises was approved and it is scheduled to be finished by the end of 2011. The authorities reported that the FIU pays special attention to its information technology system which is constantly being improved. The full list and specification of hardware and software that is on disposal to the FIU staff is provided in Annex XIX. The authorities further reported that plans for improvement of the said system have already been approved. Software MoneyWeb that will ensure communication between the FIU and obliged entities. MoneyWeb is planned to be a web portal with three layer architecture containing following modules: electronic registry being electronic bulletin as well with information on black lists, legislation, information exchange between the FIU and obliged entities, the database module and the Document Management System. The electronic registry and database module are two separate systems interconnected via standardised interfaces

[6] Authorities further reported that the Annual Report for 2010, which was published by the end of June 2011, shall include typologies and trends.

235. Apart from its core FIU functions, (receiving, analysing and disseminating UTR as well as requesting additional data) described previously in the report, the Slovak FIU is obliged by the AML/CFT Act to perform some other functions such as supervision of obliged entities

236. The FIU devotes a significant portion of its activities to supervision competence. The FIU supervises all reporting entities. Other supervisory bodies, the NBS and the Ministry of Finance notify the FIU on all their activities. The FIU is in charge of co-ordinating these activities as well as imposing all of the sanctions provided in the AML/CFT Act. Sanctions are imposed according to the general administrative procedure rules.

237. Outreach activities are also one of the priorities of the FIU.

238. The evaluators got an impression from meetings held during the on-site visit that various stakeholders in the AML/CFT system recognise the FIU as a lead authority in this field. This was observed both from the representatives of reporting entities and state authorities, which tend to rely on the FIU for most issues in co-ordinating and improving the AML/CFT system.

239. The evaluation team considers that additional measures should be taken by the authorities to adequately fund and staff the FIU. Additional technical resources would also be required. This assessment should be read particularly in conjunction with previous statements on the FIU having a lot more responsibilities and competences than those described as FIU core activities.

240. The budget for the FIU has steadily increased between 2006 and 2010. It is generally divided into 3 allocations: 1) staff costs; 2)operating and capital costs; 3) financial (special) costs. The budget of the FIU for 2011 is €1,200,000 including expenses in the amount of €250,000 for reconstruction of new premises for FIU staff. The budget for the FIU in 2010 was approx. €920,000 for 2010, €895,000 for 2009 and €847,000 for 2008.

Integrity of FIU authorities (c.30.2)

241. Employees of the FIU are police officers. They are recruited under Section 14 of the Act No. 73/1998 Coll. on the Civil Service of Officers of Police Force, the Slovak Intelligence Service, Penitentiary and Judicial Guard Force of the Slovak Republic and the Railway Police as amended, where conditions of eligibility and recruitment proceedings are stipulated. According to this section recruits should be age over 18, be respectable, be reliable, meet the requirement of general education determined for the performance of function where he is to be appointed, be capable for the performance of service from the point of view of health, physical and psychical state, accomplished basic military service or alternative service if not being subject to military service, knows state language and has permanent residence in the territory of the Slovak Republic. To be respectable for purposes of this act means that recruit was not sentenced for an intentional criminal offence. To be reliable means that recruit does not consume alcoholic beverages excessively, use addictive substances or that other facts are not revealed during recruitment that do not guarantee proper performance of civil service.

242. Requirements for their professional qualifications are having a second degree university education or university degree, preferably in law, security services and economics and previous practice within police. The staff of the Slovak FIU hold certificates issued by the National Security Bureau. They are obliged to abide by confidentiality rules as set out by the AML/CFT Act.

Training of FIU staff (c.30.3)

243. The authorities reported that the new employees recruited by the Slovak FIU are trained internally immediately upon their recruitment. The FIU staff has been stable since 2004 and received regular training within the FIU on new trends and typologies. They have also received educational input from foreign information and contacts.

244. The FIU members participated in a number of seminars and workshops organised by Europol, CEPOL or other foreign authorities in the area of money laundering and terrorist financing. (see details of trainings in the Annex XX)

Recommendation 32 (FIU)

245. The FIU is legally obliged to maintain statistics on the number of unusual transaction reports received, the particular ways of processing unusual transaction reports and their number including the number of cases submitted to law enforcement authorities or tax administrators for a calendar year and the number of persons prosecuted, the number of persons convicted of ML and the value of seized property, confiscated property or forfeited property. In this regard the FIU is authorised to request from public authorities and obliged entities all documents and information necessary to keep that statistical data.

246. The FIU maintains comprehensive statistics on unusual transaction reports, on cases opened and disseminated to competent authorities with breakdown of which authorities are provided with information, on international co-operation with foreign FIUs, on transactions postponed after receiving UTRs, on reports received form Customs on cash transfers and on feedback received from law enforcement on results of the cases disseminated by the FIU. All statistical information is maintained in a computerised database which enables it to visualise statistics with relevant breakdowns.

247. The issue of concern regarding statistics kept by the FIU is in close relation to its activities and role in the overall system. Namely, as the FIU is obliged to analyse and disseminate the cases which are related to all criminal offences, cases which may be the concern of security services, tax administration etc, the statistics maintained and provided to evaluators, do not appear to concentrate on ML or TF cases, but on all criminal offences equally. This could be useful in reviewing the system in place for combating crime in general but could be misleading in reviewing the effectiveness of the specific AML/CFT sub-system.

248. Law enforcement authorities provide some kind of feedback to the FIU regarding the cases that the FIU disseminates. This feedback concentrates on numbers of cases that are submitted to operational units and investigators to undertake their competences on the basis of the Act on Police Force or the Criminal Procedure Code. According to this data, the FIU can see the number of cases that resulted in formal investigations and eventually prosecutions. More substantive data is missing here so the FIU can see the actual background of cases e.g. whether investigation is conducted on predicate crime only or money laundering only or both, what predicate crime was involved and other facts of cases. This should especially be emphasised because the FIU disseminates cases on the basis of various legal acts and on all criminal offences, not just ML and TF.

Effectiveness and efficiency

249. Employees in the FIU have direct access to a variety of police databases and publicly available sources, which were integrated within a satisfactory IT system that is constantly being improved. This enables it to act quickly and effectively in its analytical functions.

250. The FIU employees are professional and motivated. The average time for analysing a report is 30 days with a maximum of 60 days in complex cases (which is also monitored by the IT system).

251. The AML/CFT Act requires the FIU to disseminate cases to law enforcement bodies which relate to all criminal offences, not just the ML and TF. A large number of cases that are analysed and disseminated to law enforcement authorities, are disseminated in accordance with the letter (a) of Section 26 of the AML/CFT Act, which requires the FIU to disseminate any indication of any criminal offence. In all of these cases there is no need for a clear link to ML or TF (See paragraph 255 above). This work is done by the FIU as an integral part of the Police force. This fact highlights the issue of non-specificity of the FIU in the overall police structure, which in the view of the evaluators, is unfortunate. In the situation where the FIU is in charge of the system itself, and where the effectiveness of prosecution and adjudication of ML cases is of the major concern, the FIU is the body that should take the responsibility of generating the cases that would lead to convictions for serious ML cases. Especially, internet fraud activities like phishing and pharming take significant place in the FIU's daily work. Moreover, the FIU is obliged to inform tax authorities on possible tax evasion cases, and to maintain a separate database of information extracted from UTR, which is made available to Security Services in Slovakia. Although Slovak authorities are firm in the position that the FIU as police unit cannot concentrate on just a few specific criminal offences and that the fact that the FIU analyses and disseminates information on all criminal offences equally can only be the benefit or advantage in FIU work, evaluators are still on the position that all these additional requirements do not allow the FIU to concentrate sufficiently on ML and TF, which in the view of the evaluators should be the main focus. This raises concerns about the effectiveness of the overall AML/CFT system in place, especially bearing in mind that the AML/CFT Act itself puts the FIU in the centre of that system, thus putting on it the factual responsibility for co-ordination and development of the whole system. The FIU shows a very high level of dedication to its responsibilities in this sense, but it is arguable whether this goal could be achieved with present level of resources and its position in the overall police structure and AML/CFT system as a whole.

252. Data presented above not only related to ML offences they are related to all offences that have been analysed and disseminated by the FIU on other predicate offences. Data specifically related to ML could not be provided. This table is prepared by the Slovak authorities and should be read in conjunction with paragraphs 215 and 216 of the report, which state that approximately 20% of disseminated cases relate to ML. Statistical data from 2009 is more comprehensive than previously due to legislative requirements to keep statistics. The table also shows that the FIU does not disseminate cases to the prosecutor's office directly, but only to different departments of the Police force. There is no link between the number of indictments and the figure (0) of disseminations to prosecutors. The FIU can only receive the feedback on number of indictments which have gone through police channels. Information on autonomous ML indictments could not be provided by the authorities, as this information is not kept by the FIU. From the statistics presented below it is very hard or even impossible to establish ultimate effectiveness of the AML/CFT system that results from UTRs. Unfortunately, the authorities were not able to demonstrate how many convictions, if any resulted from UTRs. The FIU estimated that about 200 police cases in 2010 were originated by UTR system, which were said to relate to fraud, tax offences and drug trafficking. The outcome information however was not available.

Table 12: Statistics on notifications and judicial proceedings relating to UTRs

	2006		2007		2008		2009		2010 (to June)	
	ML	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**
Number of STRs	1,457	14	1,910	10	2,157	16	2630	56	2415	55
Cases opened by the FIU	1,556	14	1,936	9	2,258	16	2630	56	2415	55
Notifications to law enforcement (police)	N/A	N/A	N/A	N/A	N/A	N/A	805	56	761	55
Notifications to prosecutors	N/A	N/A	N/A	N/A	N/A	N/A	0	0	0	0
Notifications to tax authorities	N/A	N/A	N/A	N/A	N/A	N/A	412	0	549	0
Number of indictments based on UTRs	N/A	N/A	N/A	N/A	N/A	N/A	68	0	4	0
Number of persons indicted on the basis of UTRs	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Number of convictions based on UTRs	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Number of persons convicted on the basis of UTRs	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

* N/A = Not Available

2.5.2 Recommendations and comments

Recommendation 26

253. The AML/CFT Act defines the FIU as national unit for the area of prevention and detection of money laundering and terrorist financing. This provision is supposed to enable the FIU to be the leading national authority in this matter and also the overall co-ordinating body of the various state bodies in the different parts of the system. The FIU is gradually becoming the leading player in the system. It makes impression of a proactive and diligent institution which could take the leadership role. Nonetheless, the FIU continues to have a rather weak formal position in the current police structure.

254. The new AML/CFT Act describes in detail the competences of the FIU, but it does not resolve the issue of its status. Significant work has been done by the FIU since the 3rd round evaluation, but still, the main issues remain have not been completely resolved. It is work in progress and authorities should focus more on resolving them. The evaluators continue to have concerns about the strength of the unit, given its organisational position in the Police structure, to bring together all the ministries and other state bodies in order to ensure the system works effectively. Concerns regarding operational independence and autonomy remain unresolved from the 3rd round evaluation, as formal legal safeguards to protect the operational independence of the director of the FIU have not been put in place. Therefore, Slovak authorities should introduce formal safeguards to ensure the FIU's operational independence and autonomy.

255. The FIU's position in the police structure and in the AML/CFT system as a whole should be revisited.

256. The FIU should be encouraged to concentrate more on ML and TF cases. At the moment a lot of resources are employed to analyse internet fraud, predicate offences and tax evasions. It is recognised that there can be a clear benefit of the work of the FIU in fighting crime generally, especially dealing with various forms of predicate criminality, where the FIU is tracing and detecting the criminal assets through the investigations of the predicate offences. If the FIU is concentrating on the predicate offences the evaluators would expect some positive results on the confiscation side. Unfortunately this has not been demonstrated. Thus in the absence of meaningful statistics which can show results, serious doubts exist on the effectiveness of the system in fighting proceeds–generating crime generally.

257. The FIU should continue with its activities in publication of periodic reports. These reports should include information on trends and typologies.

Recommendation 30

258. The FIU needs more resources both human and material, especially due to the fact that the FIU is widely seen as a lead player in AML/CFT area. Almost all other stakeholders met on-site, both state bodies and reporting entities mentioned the FIU in this sense, thus relying on the FIU to promote the development of the system.

259. The FIU is vested with the whole range of tasks beyond its core functions, e .g. supervision of reporting entities, outreach to the financial sector and DNFBPs, awareness raising and training activities, drafting legislation and guidelines etc. All of the departments should be strengthened, especially the UTR and the Supervision Departments.

260. Outreach to the financial sector and DNFBPs is seen as one of the priorities of the FIU work. The FIU has done a lot in this regard since the 3rd round evaluation bearing in mind the level of resources allocated. More substantial resources should be allocated to the FIU for these purposes.

Recommendation 32

261. The AML/CFT specific statistics should be collected regularly apart from statistics on all criminal offences which are subjects of interest of the FIU.

262. More substantive feedback from law enforcement bodies on ML or TF cases is needed in this regard.

2.5.3 Compliance with Recommendation 26

	Rating	Summary of factors relevant to s.2.5 underlying overall rating
R.26	**PC**	• Concerns over 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 should contain information on trends and typologies. • The FIU does not concentrate sufficiently on ML and TF which should be the main focus, but rather on all criminal offences equally. • Effectiveness of the FIU work on specific ML/FT cases cannot be appropriately established since statistics relate to all criminal offences.

2.6 Cross Border Declaration or Disclosure (SR.IX)

2.6.1 Description and analysis

Special Recommendation IX (rated PC in the 3rd round MER)

263. Slovakia was rated partially compliant in the 3rd round MER stating that the declaration system had been introduced just before the on-site visit and that Slovak authorities were not aware of those provisions. It was recommended that the Slovak authorities should take necessary measures to ensure effective compliance with SR IX. At that time Slovakia had a domestic system put in place by the Act on Customs, which had not been fully considered, pending completion of the relevant EU legislation.

264. The cash control system in Slovakia is based on the Regulation (EC) 1889/2005 of the European Parliament and of the Council of 26 October 2005 on Controls of Cash Entering or Leaving the Community (hereinafter: Cash Control Regulation), which came into force on 15th June 2007. As an EU Member State this Regulation is directly applicable in Slovakia to cross-border transportation of currency and bearer negotiable instruments at its borders with non-EU countries.

265. In addition to the Cash Control Regulation, there are several other laws in place which are used in Slovakia in order to implement the requirements of SR IX. The Act No. 199/2004 on Customs Law and on Amendments and Supplements to Some Acts (hereinafter: Customs Act) and the Act No. 652/2004 on State Administration Bodies in the Field of Customs and on Amendments and Supplements to some Acts (hereinafter: Customs Bodies Act) which have been provided to the evaluators during the course of the on-site visit.

266. As advised by the authorities, the Cash Control Regulation is directly applicable while the other two mentioned Acts deal with specific issues not covered by the Cash Control Regulation. For the purpose of this report the evaluators regarded the EC Cash Control Regulation and the Customs Act as the legal basis for the cross-border declaration system in Slovakia. Subject to the footnote below the evaluation team have assessed the compliance of the Cash Control Regulation and the Customs Act with the FATF standards as well as their implementation in Slovakia with an increased focus on effectiveness.[7]

267. Article 3 of the Cash Control Regulation establishes an obligation to declare cash in the value of €10,000 or more when entering or leaving the EU space. This obligation meets the prescribed threshold in the essential criteria which cannot exceed €15,000. The Regulation prescribes that an incorrect or incomplete declaration cannot be taken to mean that the obligation is fulfilled.

[7] MONEYVAL discussed the evaluation of SR IX in its EU Member States in the follow up round during its 35th plenary meeting in April 2011. MONEYVAL noted that under the supranational approach, there is a pre-condition for a prior supranational assessment of relevant SR IX measures. It further noted that there is as yet no process or methodology for conducting such an assessment (although one is planned). Pending the FATF's 4th round, as an interim solution, MONEYVAL agreed that it will continue with full re-assessments of SR.IX in the 6 remaining EU countries to be evaluated (which includes Slovakia). These countries will be evaluated using the non-supranational approach. Nevertheless, it noted that, for the purpose of Criterion IX.1, the EU has been recognised by the FATF as a supranational jurisdiction and therefore there is no obligation to comply with this criterion for intra-EU borders. Downgrading solely for the lack of a declaration/disclosure system is thus not appropriate. The other criteria that mention supranational approach (C.IX.4, C.IX.5, C.IX.7, C.IX.13 and C.IX.14) would not be evaluated against the requirements that apply to the supranational approach, and C.IX.15 would not be evaluated. The FATF was advised of this solution as it involves a departure from the language of the AML/CFT Methodology. At its plenary meeting in Mexico in June 2011 the FATF took note of this interim solution for EU Member States in MONEYVAL's follow up round.

268. Article 2 of the Cash Control Regulation defines "cash" as including currency and bearer negotiable instruments including monetary instruments in a bearer form (such as travellers cheques), negotiable instruments that are either in a bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such a form that the title thereto passes upon delivery as well as incomplete instruments (such as promissory notes and money orders) signed but with the payee's name omitted.

269. Paragraphs (1) and (2) of Section 4 of the Customs Act provides for an obligation to report on the import, export, and transit of pecuniary means or other means of payment in following the manner:

"Import, export, and transit of pecuniary means in cash or other equivalent means of payment across the customs area of the Union is subject to customs supervision. Other equivalent means of payment are understood to be securities, cheques and bills of exchange, precious metals, and precious stones."

270. A person who imports, exports or transits pecuniary means in cash or other equivalent means of payment pursuant to paragraph 1 in the total amount equivalent to an amount of at least €10,000 is obliged to report this fact to the relevant Customs Office in writing in a form. (Section 4 of the Customs Act)

271. Nevertheless, it is unclear to the evaluators which Act is implemented in practice. Both pieces of legislation are in force and both stipulate a similar obligation of establishing a cash declaration system but some inconsistencies exist between them.

272. An inconsistency appears to exist regarding reporting forms, which are used in practice. Slovak authorities indicated that reporting forms are made available to passengers on the borderlines, and that is the National Declaration Form provided in the Customs Law. The so-called the "Common Declaration Form" that was elaborated within the Cash Control Working Group of the European Commission, which, at the same time, is used by the rest of the EU Member States in their respective languages is still not used in practice. However, as advised by the authorities, the Customs Authority intends to use the CDF worked out by Cash Controls Working Group. They have also reported that the implementation requires fulfilment of two conditions: the updated CDF which should be a result of one of the PG "B" for Cash Controls "Elaboration of an EU CDF and its implementation" and legislative amendments to the annex 01 to the Customs Act. The form given in the Customs Act does not correspond to the form annexed to the Cash Control Regulation. Although authorities clarified that only one reporting form is used in practice (as provided in the national legislation) the legal issue remains that the Cash Control Regulation is directly applicable in the Slovak Republic as the integral part of the EU but in parallel with the national legislation dealing with same issues (Customs Act).

273. The Customs Act provides for the obligation to make a declaration also in cases of "sending to a third country or receiving from a third country a postal item or other consignment containing pecuniary means in cash or equivalent means of payment to a total amount equivalent to an amount of at least €1,000".

274. With regard to obtaining further information from the carrier regarding the origin and intended use of the currency and bearer negotiable means, the customs offices are able to exercise the control of performance of the declaration obligation. In the event of control, the customs office is authorised to require the necessary co-operation from controlled persons. The customs office exercises control in accordance with authorisations and with the application of means pursuant to a specific regulation. This specific regulation is to be understood as the Customs Bodies Act No.

652/2004, which specifies competences of administrative bodies in customs related issues. Section 17 of the said act states *that "customs officer is authorised to request necessary explanation from the person that may contribute to clarification of the facts necessary for uncovering a customs offenc*e…" This includes non-declaration or false declaration of cash. Furthermore, the same section states that *"In case of need, customs officer is authorised to call on a person to present it at once or at a given time to the customs office for the purposes of drawing up a record and explaining itself."* Effectiveness of the implementation of this provision with regard to declaration system cannot be assessed due to absence of cases where a false declaration or failure to declare has been discovered.

275. With regard to the authority of competent bodies to stop or restrain currency or bearer negotiable means, Slovak authorities rely on provisions of Section 22 of the Customs Bodies Act No. 652/2004 which deals with "Authorisation for Detention of an Article" in the following manner: "if there is a justified suspicion that an article, goods or papers connected with a criminal offence or misdemeanour committed in connection with infringement of customs regulations or violation of customs law pursuant to a specific regulation (including non-declaration or false declaration of cash), or with infringement of tax assessments and if it is necessary for finding out the facts, the customs officer is authorised to detain them for the execution of necessary operations. The detention may last for 60 days." Again, due to the absence of any case of failure to declare or false declaration, effectiveness of this provision cannot be established.

276. Any recorded cases of cash controls at border customs offices, be it an orderly record of a declared amount or a case of false declaration/undeclared cash detected, will remain at the disposal of the customs and the FIU for possible future reference normally for 5 years, and then they are archived.

277. Information obtained by customs authorities is provided to the FIU once per month. Paragraph 5 of Section 4 of the Customs Act states that *"The Customs Office sends the completed forms pursuant to paragraph 2 and notifications on infringement of customs regulations pursuant to Section 72 Par. 1 letter n) to the Financial Police Service of the Police Force by the fifth day of the calendar month following the month in which these facts occurred."*

278. The Slovak FIU obtained five reports in 2009 in a total amount of €124,500 from the Customs Authority of the Slovak Republic related to transport of funds on enter from Ukraine to Slovakia. In all those cases, transport of funds in cash in EURO was carried out by Ukrainian citizens declaring that the purpose of funds was to purchase a van in two cases, to purchase a car in two cases and to purchase consumer goods in one case. Germany was declared as a destination country for the purchases. Declared purposes of purchases were verified by the Slovak FIU with the following results: in one case the declared purchase was actually fulfilled - the vehicle was bought in Germany and transported through the Slovak Republic to Ukraine. In other cases no transport of goods from the Slovak Republic to Ukraine was recorded. The FIU used these reports from Customs Authority in a same way as it uses unusual transaction reports sent by reporting entities.

279. From the information received on-site, it is noted that the Customs Administration sent 22 cash declarations in the period form 1 January 2010 to 20 September 2010. In 20 of these cases Ukrainian citizens declared the funds at the border, stating the purpose of buying a motor vehicle.

280. No cases of false declaration have yet been recorded by the Slovak authorities.

281. The Slovak authorities reported in the MEQ that the co-ordination between customs, police and immigration authorities on the national level is executed within the Interagency Integrated Group of Experts. This group consists of the representatives of the FIU, the NBS, the Ministry of Finance, the Tax Authority, the Specialised General Prosecutor's Office, the General Prosecutor's Office, the Ministry of Justice, the Customs Authority, the Unit of Combating Terrorism of the

BCOC, the National Anti-Drug Unit of the BCOC and the Bureau of Justice and Criminal Police of Presidium of the Police Force meets usually three times per year and deals with policy issues related to the AML/CFT. The operational co-operation and co-ordination between authorities present at borders does not seem to be sufficient when it comes to the cash control. The border police would normally notify the Customs Office if some goods or merchandise are discovered during the security checks, but not the cash or bearer negotiable instruments. If cash or bearer negotiable instruments are found, the police would start their own investigation, if a suspicion exists on a possible criminal offence.

282. The Convention on mutual assistance and co-operation between customs administrations, so called Naples II Convention, is commonly used in the international co-operation. As an EU Member State Slovakia also applies the EC Regulation 515/97 on mutual assistance in customs matters.

283. Within the EU, law enforcement sensitive information is shared between customs both via formal and informal channels (bearing in mind the time factor in the latter case). An important element of exchanging cash control related information is the platform set up by the EU Commission which is the Cash Control Working Group with participants of customs officials of every EU Member State, convened on a regular basis. The RIF system is accessible to all EU Member States' customs authorities thus ensuring the timely and prompt access to all cash control related suspicious cases, trends.

284. Information on suspicious cash movements are recorded and stored in the RIF system, which is accessible to all customs services throughout the EU. In case of third countries, information can be exchanged on request by competent authorities of either third countries or their Slovak counterpart if rules of professional confidentiality, bilateral agreements and data protection so allow.

285. The Slovak Customs Authorities regularly receive information from other member states about new trends and seizures in the field of cash transfers. This co-operation is informal but very useful. Slovak Customs Authorities have participated at the international control operations focused on the illegal money transfers, money laundering and terrorist financing. They reported that they had involved in the operation ATLAS, which focused on the physical cross-border transportation of currency or bearer negotiable instruments and took place in October 2009 at international airports.

286. It is left to the Member States by the Cash Control Regulation to lay down penalties, which under Article 9 have to be effective, proportionate and dissuasive. Section 72 of the Customs Act No. 199/2004 states that a violation of customs law or customs offence is committed by the one, who does not fulfil the obligation to report cash or bearer negotiable means pursuant to Section 4 of the same act. The Customs Office is the body that is competent for imposing sanctions, which include fine and forfeiture of goods or an article.

287. A fine up to €99,500 may be imposed for violation of customs law according to the gravity of violation of customs regulations. A fine imposed for violation of customs law is payable within 30 days from the day when the decision by which it was imposed comes into force. The forfeiture of goods or an article may be imposed, if the goods or an article in the property of a perpetrator were used or designated for committing violation of customs law or were acquired through violation of customs law, or were acquired for goods obtained through violation of customs law. The forfeiture of goods or an article may be imposed, if the value of goods or an article is in an obvious imbalance to the nature of violation of customs law. The forfeiture of goods or an article may be imposed independently or together with a fine.

288. Sanctions provided in the Customs Act are generally applied for all so-called customs offences such as illegal import or export of goods, avoiding customs supervision, including the false

declaration or the failure to declare. The fine which can be imposed is also given in general as a maximum penalty for all customs offences and it is up to the customs office to determine the gravity of specific acts. Since no penalties have been imposed for failure to declare or false declaration of cash and other bearer negotiable means yet, the evaluators are not in a position to assess whether these sanctions are effective, proportionate and dissuasive. In other words, there is no practice established by the customs authorities with regard to penalties for false declaration or failure to declare and in the absence of specific penalties prescribed for these violations it is impossible to assess whether the sanctions are in line with the international standards.

289. Forfeiture of articles or goods is also used in customs usual work but it is arguable whether this sanction can be imposed in relation to cash controls, especially bearing in mind the provision which states that forfeiture of goods or an article may be imposed, if the value of goods or an article is in an obvious imbalance to the nature of violation of customs law.

290. Overall, the effectiveness of the sanctioning regime cannot be established.

291. Physical cross-border transportation of currency or bearer negotiable instruments that are related to TF or ML is considered as a crime according to the Criminal Code. If it is established that currency or bearer negotiable instruments are proceeds from, instrumentalities used in or instrumentalities intended for use in the commission of any money laundering, terrorist financing or other predicate offences this Act. As a result, sufficient evidence should be available for initiating criminal proceedings. It should be noted that questions on confiscation, freezing and seizing of proceeds related to money laundering or terrorist financing discussed under Recommendation 3 apply accordingly to situations involving cases related to SR IX.

292. As advised by the customs authorities, they receive the lists of terrorists from the Ministry of Foreign Affairs regularly. Authorities, however, could not specify the legal basis of this practice and the frequency of receiving of the lists from the Ministry of Foreign Affairs. Customs officers check these lists whenever export to some countries that are considered more risky occur. Issues and consideration stated earlier in the report in relation to SR III also apply to SRIX.

293. Authorities advised that notification of suspicious or unusual cross-border movement of gold, precious metals or precious stones can be provided as spontaneous information in the framework of Naples II Convention or in a framework of a bilateral agreement, or through Europol or Interpol. However, no such a case has been recorded.

294. Systems for reporting cross border transactions are subject to the Act No. 428/2002 on Protection of the Personal Data. There seem to be strict safeguards in place to ensure proper use of the data that is reported and recorded.

295. With regard to the training activities, Slovak authorities rely on basic customs training. In the scope of this basic customs training, customs officers are receiving training on cash control, as it is an integral part of the customs law. Awareness raising activities are undertaken as a part of already mentioned joint customs operations with customs authorities of other EU Member States. No specialised training in the area of control of cash and other bearer negotiable means or combating ML and FT is available to customs officers yet.

296. Customs authorities met on-site advised the valuators that the customs criminal offices, which exists in the structure of the Customs Administration, concentrate on investigations of criminal offences closely related to illegal cross border activities such as smuggling and drugs trafficking. Cross-border transfer of money is not the priority at the moment. If money is discovered during investigations of customs related offences, the case would normally be transferred to the financial police for investigation due to practical difficulties in providing evidence. The evaluators noted that

the co-ordination and co-operation in this kind of cases are at a very low level. Customs offices do not concentrate on possible ML or TF cases. Furthermore, regular controls of passengers are done on arrivals but rarely on departures. The same goes for export and import of goods where imports are checked but not the exports. No specific indicators for customs officers are developed in order to recognise possible ML or TF on borders nor is specific training provided in this sense, while the awareness raising is still in the initial phase.

297. The evaluators were advised that passengers at borders are informed on their obligation to make declarations by posters, which are placed on every border crossing. It appears that arriving air passengers are not supplied with a declaration form prior to landing, and are not otherwise advised prior to arrival of their obligation to make a declaration. These measures should be reconsidered in the light of very poor reporting of cash and other bearer negotiable instruments, in order to ensure that travellers are aware of their obligation to declare these instruments.

Additional elements

298. From what has been seen on-site and from the MEQ, it seems that Slovak authorities pay little attention to the implementation of the measures set out in the Best Practices Paper for SR.IX.

299. Reports are maintained in a computerised database.

Recommendation 30 (Customs authorities)

300. The total number of customs staff employed on customs activities – physical controls of goods entering or leaving EU – is as follows:

Customs Office (CU)	Place	Number	Customs branch
CU Bratislava	Bratislava	6	airport
CU Trnava	Piešťany	6	airport
CU Poprad	Poprad	6	airport
CU Žilina	Dolný Hričov/Žilina	6	airport
CU Košice	Košice	13	airport
CU Michalovce	Čierna nad Tisou	38	railway
CU Michalovce	Vyšné Nemecké	102	road
CU Michalovce	Ubľa	42	road
CU Michalovce	Veľké Slemence	12	road

*the available number of the customs officers on a given day is one quarter from total number of staff and customs officers are responsible for carrying out of the all physical controls (not only cash controls).

Recommendation 32

301. Comprehensive statistics are maintained regarding declarations made by travellers as described above. However, there are no statistics on cases of false declarations or failure to declare, nor on suspicious cases of possible money laundering or terrorism financing, but this issue is attributed to the effectiveness of the system itself, not to the statistics maintained. Both customs authorities and the FIU hold these statistics. Five reports in 2009 and 22 reports on cross border transportation of currency in the period from 1 January 2010 to 20 September 2010 were recorded.

Effectiveness and efficiency

302. Although the Slovak authorities seem to comply with some of the criteria under the SR.IX, some deficiencies remain, as noted above.

303. The very low number of declared transfers of cash or other bearer negotiable raises concerns on the effectiveness of implementation of the declaration system. Moreover, no cases of false declarations or failure to declare have been recorded. The Slovak authorities should take urgent measures to establish reasons for this situation and to address the issue in appropriate manner.

304. It seems that little or no attention has been given to the actual implementation of the requirements of SR IX. No specific measures have been undertaken in order to detect possible cash movements. No indicators or other forms of guidelines have been provided to customs officers in order to enable them to recognise possible cash movements or suspicion of possible ML or TF, no effective co-operation between customs and other state bodies presented at borders, no regular scrutiny of passengers on departures or goods in exports. Movements of cash are subject to work of customs office only in cases when cash is discovered in other actions performed, such as house or baggage searches and even then, cases would be transferred to the police for investigation.

305. No sanctions have yet been imposed. Bearing in mind that sanctions in the Customs Act are given in general terms for all customs offences, it is crucial that some practice is established for specific offences of false or non-declaration. The effectiveness of the sanction regime thus cannot be established.

306. There are no ML/TF investigations triggered from cross-border cash declarations nor are customs officers provided with guidance regarding indicators neither for recognising possible ML or TF nor on procedures to follow when an illegal or suspicious transfer is discovered.

2.6.2 Recommendations and comments

307. Slovak authorities should remove all inconsistencies that exist in the legal framework so as to avoid legal uncertainty with regard to the implementation of SR IX. Although, inconsistencies in the legal framework regarding declaration forms can be considered as a minor flaw, the system could only benefit from the existence of just one reporting form in place.

308. Slovak authorities should take steps to raise awareness of arriving and departing travellers by making the sign alerting travellers to the requirements at ports of entry and exit much more visible, and perhaps in several languages.

309. Specialised training activities related to SR IX for the staff of the customs administration should be organised.

310. Slovak authorities should take steps to heighten the awareness of customs officers and all other competent bodies present at borders (e.g. police, immigration office) of the obligations arising from SR IX. Also, clear and effective mechanisms and procedures should be developed for the daily operational co-operation and co-ordination in exchange of intelligence and other information between all bodies present at the borders.

2.6.3 Compliance with Special Recommendation IX

	Rating	Summary of factors underlying rating
SR.IX	**PC**	• Inconsistency regarding reporting forms exist in the legal framework due to the existence of two pieces of legislation dealing with the cash

		reporting system (one on the EU level and one national). • The system itself is rather ineffective since there are a very low number of declared transfers, no cases of false declaration or failure to declare, no cases of ML or TF triggered by the system and no sanctions imposed for false declaration. • Deficiencies in the implementation of SR III may have an impact on the effectiveness of the regime.

3 PREVENTIVE MEASURES - FINANCIAL INSTITUTIONS

311. In Slovakia, the preventive measures of the AML/CFT system were primarily regulated in the Act No. 367 of 5 October 2000 on protection against legalisation of incomes from illegal activities and on amendment of some acts. As an EU Member State, Slovakia was required to implement the Third EU AML/CFT Directive (Directive 2005/60/EC) and the implementing Directive 2006/70/EC) into its national legislation. The Act No. 297/2008 Coll. of 2 July 2008 on the Prevention of Legalisation of Proceeds of Criminal Activity and Terrorist Financing and on Amendments and Supplements to Certain Acts as amended by the acts No. 445/2008 and No. 186/2009 entered into force on the 1st September 2008 (hereinafter referred to as "AML/CFT Act") (See Annex III). This Act implements the Third EU AML/CFT Directive in Slovakia, and stipulates the basic rights and obligations of legal entities and natural persons in the prevention and detection of legalisation of proceeds of criminal activities and terrorist financing. It has removed many gaps identified in the 3rd round MER relating to the Slovak AML/CFT regime.

312. The scope of financial institutions covered is determined by Section 5 of the AML/CFT Act as follows:

a) a credit institution,
b) a financial institution, other than a credit institution, such as
   1. the Central Securities Depository,
   2. a stock exchange,
   3. a commodity exchange,
   4. an asset management company and depository,
   5. a securities dealer,
   6. a financial agent, a financial adviser,
   7. a foreign collective investment entity,
   8. an insurance company, reinsurance company, insurance broker, reinsurance broker,
   9. a pension asset management company,
   10. a supplementary pension insurance company,
   11. a legal entity or a natural person authorised to perform exchange of foreign currency or wireless foreign currency transfers or to provide foreign exchange services, finance lease or other financial services under a special regulation,
c) the Export-Import Bank of the Slovak Republic.

313. A branch, an organisational unit or a place of business of an above-mentioned foreign legal entity or a natural person, including a representative office of a foreign credit institution and a representative office of a foreign financial institution which operate in the territory of the Slovak Republic are also listed in the same Section as obliged entities for the purposes of this Act.

314. The basic obligations under the AML/CFT Act cover:

- Customer due diligence;
- Detection of an unusual transaction;
- Refusal of establishment of a business relationship, termination of a business relationship or refusal of carrying out transaction;
- Postponement of an unusual Transaction;
- Reporting of "unusual" activity to the FIU;
- Obligation of keeping secrecy about a reported unusual transaction;
- Data processing and record-keeping;
- Preparing in writing and updating its own activity programme aimed at the prevention of Ml and TF.

315. Since the adoption of the 3rd round MER there have been important changes in the supervisory structure for financial institutions in Slovakia. Since January 2006, the NBS is the single supervisory authority over the financial market in the Slovak Republic. The general procedural rules followed by the NBS in supervising and regulating the financial market in the areas of banking, capital market, insurance and pension savings are laid down in the Act No. 747/2004 Coll. on Supervision of the Financial Market and on amendments to certain laws as amended (hereinafter referred to as "FMS Act"), which entered into force on the 1st January 2006.

316. Besides, since 1 July 2010 some changes in the organisation of the Financial Market Supervision Unit have been approved by the Bank Board of the NBS; thus, this unit is directly under the authority of an executive director with 3 departments:

- Supervision over banking sector and payment services providers (including FX offices),
- Supervision over the securities, insurance and pension markets,
- Regulation and financial analysis (including banking and payment services regulation section, which among other responsibilities encompasses also the prevention of ML/TF in financial market).

Customer Due Diligence and Record Keeping

3.1 Risk of money laundering / financing of terrorism

317. The evaluators were not advised of any formal AML/CFT risk assessment undertaken since the last evaluation. Nonetheless, they were advised that there is a significant threat from domestic organised crime investing its proceeds overwhelmingly within the Slovak economy. The authorities consider the TF risk to be low.

318. By implementing the Third EU AML/CFT Directive the Slovak Republic adopted and implemented also the risk-based approach, particularly in relation to customer/beneficial owner identification and verification requirements. Pursuant to the AML/CFT Act obliged entities should determine the extent of CDD measures on a risk-sensitive basis and apply it to all their customers. Obliged entities consider the risk of ML or TF for the purpose of this Act with regard to the customer, type of transaction, business relationship or a particular transaction. It is worth mentioning that due to the fact, the most significant players in the banking sector are majority owned by foreign financial groups, the implementation of the risk-based approach standards throughout the sector can be deemed swift and comprehensive.

319. The AML/CFT Act requires obliged entities to perform enhanced due diligence if, according to the information available, some of the customers, some types of transactions or some particular transactions represent a higher risk of ML or TF. In the case of enhanced due diligence, obliged entities are required to perform, in addition to normal CDD measures, further measures depending on the ML or TF risk. Enhanced due diligence is required in any case for non face-to-face business relationships, cross-border correspondent banking and PEPs. Those three enhanced risk-categories are modelled on the risk-based approach set out in the Third EU AML/CFT Directive and appear not to be the result of a specific risk-based approach.

320. Based on the instances provided by the Third EU AML/CFT Directive Slovak Law allows for simplified CDD where the customer is a financial institution which conducts its activities within the territory of the EU or in a third country that imposes equivalent AML/CFT requirements, where the customer is a company listed on an EU regulated market or a company from a third country that imposes disclosure requirements consistent with EU standards or where a customer is a specific domestic public or EU authority or agency (see c.5.8 for further details).

321. The NBS uses a risk matrix to conduct proper supervision activities according to their risk profile. Supervisory cycle is at maximum two years depending on a risk profile of the supervised entity.

3.2 Customer due diligence, including enhanced or reduced measures (R.5 to R.8)

3.2.1 Description and analysis

Recommendation 5 (rated PC in the 3rd round MER)

322. As described in the 3rd round MER, Slovakia was rated "*Partially Compliant*" for Recommendation 5 since some of the essential criteria were not provided for in the Slovak law. Comprehensive legislative amendments were made in the preventive AML/CFT system since the adoption of the 3rd round MER. In particular, the new AML/CFT Act now basically regulates due diligence measures and the identification of beneficial owners. It has significantly changed the CDD requirements for all the reporting entities – credit institutions, financial institutions, insurance and securities sector and DNFBPs as well. Therefore, Recommendation 5 has been reviewed again according to all the criteria of the Methodology.

Anonymous accounts and accounts in fictitious names (c.5.1)

323. Section 24 (2) of the AML/CFT Act obliges credit institutions and financial institutions to refuse establishing a business relationship or carrying out a particular transaction or a type of a transaction that maintains the customer's anonymity. Furthermore, the AML/CFT Act requires financial institutions to perform identification of a customer and verification of his identity.

324. Paragraph 1 of Article 89 of the Act No. 483/2001 Coll. on Banks obliges a bank or branch office of a foreign bank to refuse to conduct transactions for clients on an anonymous basis. However, paragraph 4 of the same article does not require a bank or a branch of a foreign bank to demand proof of the customer's identity in the following cases, where a customer uses an amount not exceeding €2,000:

a) in transactions carried out through currency exchange machines;
b) within the provision of financial services at a distance;
c) when using a deposit other than to establish a deposit.

325. According to paragraph 6 of Article 47 of the Act No. 8/2008 Coll. of 28 November 2007, on Insurance, "*The insurance company, branch of an insurance company from another Member State, branch of a foreign insurance company, the financial agent within the insurance or reinsurance sector and a financial adviser within the insurance or reinsurance sector shall be obliged to refuse to conclude an insurance contract within life assurance while maintaining anonymity of the client*". A similar obligation is set out in paragraph 3 of Article 73 of the Act on Securities and Investment Services ("a stock brokerage firm shall decline any transactions in which the client remains anonymous").

326. The AML/CFT Act establishes in paragraph 1 (a) of Section 10 that "customer due diligence shall include the identification of a customer and verification of his identification". Identification should be done for every "transaction" which is a concept defined as the establishment, change or termination of a contractual relationship between an obliged entity and its customer and any business operation of a customer or on behalf of a customer or disposal of property of a customer or on behalf of a customer which relate to activity of an obliged entity including an operation carried out by a customer on behalf of his own name and his own account (Section 9 (h) of the AML/CFT Act).

327. Since 1 September 2001, the opening of new bearer passbooks has been prohibited (according to Slovak Civil Code). Concerning the pay outs of bearer deposits regime, a passbook holder has the right to be paid out until 31 December 2011, when the commitment to pay out outstanding amounts will elapse. The Ministry of Finance will pay out a bearer of a passbook or a bearer of other bearer securities on condition that identification is done. Afterwards, no claim for repayment will be accepted by the Ministry of Finance in line with the Section 879 (4) of the Act No 40/1964 Coll. Civil Code.

328. According to the Agreement between the Ministry of Finance of the Slovak Republic, the State Treasury and the banks and the branches of the foreign banks which had in their evidence the balances of the cancelled bearer deposits ("Paying banks"), the State Treasury and the referred Paying banks have been empowered by the Ministry of Finance to pay out the compensations of the balances of the cancelled bearer deposits in the case of passbook holders who had not claim the deposits in due time.

329. As the evaluators of the previous round, this round's evaluation team was also advised by the authorities that numbered accounts have not been used in Slovakia though there is no explicit prohibition on this point other than the requirements set out in the Act on Banks and the Civil Code.

330. According to paragraph 1 (a) of Section 10 of the AML/CFT Act, obliged entities are required to identify the customer and verify his identification, so the financial evaluators concluded that the Slovak legal framework sets out enough identification requirements to prohibit the establishment of anonymous accounts or accounts in fictitious names. Authorities reported that due to the identification and verification requirements in the legislation in practice accounts in fictitious names have never existed in the country.

Customer due diligence

When CDD is required (c.5.2)*

331. According to paragraph 2 of Section 10 of the AML/CFT Act, obliged entities are required to perform CDD measures:

- at the moment of establishment of a business relationship;
- when carrying out an occasional transaction outside a business relationship worth at least €15,000 regardless of whether the transaction is carried out in a single operation or in several linked operations which are or may be connected;
- if there is a suspicion that the customer is preparing or carrying out an unusual transaction, regardless of the amount of the transaction;
- when there are doubts about the veracity or completeness of customer identification data previously obtained;
- where concerning withdrawal of a cancelled final balance of bearer deposit.

332. Obliged entities are also required to identify the customer and verify that customer's identity in case of carrying out a transaction the amount of which reaches at least €2,000 unless any of above-mentioned cases apply (paragraph 3 of Section 10 of the AML/CFT Act).

333. As noted above, whilst paragraph 2 of Section 10 of the AML/CFT Act imposes a CDD obligation to obliged entities when carrying out an occasional transaction outside a business relationship worth at least €15,000, Article 89 (paragraphs 1 and 4) of the Act on Banks provides a stricter identification requirement at or above €2,000 (with the exception of account opening where there is no threshold). In addition, paragraph 5 (c) of Article 13 of the Foreign Exchange Act requires the identification of the customer for each transaction in foreign exchange assets in

bureaux de change and for each foreign exchange service in excess of €1,000, unless a separate Act stipulates otherwise.

334. Pursuant to Regulation (EC) No 1781/2006 (transposing SR VII), which is directly applicable in all EU Member States, financial institutions in Slovakia must also identify the customer and ensure that complete originator information is included in cross-border wire transfers (see write-up under SR VII for more details).

Identification measures and verification sources (c.5.3)*

335. Customer identification rules are laid down in Sections 7, 8 and 10 of the AML/CFT Act. According to paragraph 1 of Section 10 the AML/CFT Act, CDD includes identification of a customer and verification of that customer's identity. Paragraph 6 of the same section further specifies that all obliged entities shall verify identification of the customer being a natural person and identify each person acting on behalf of the customer being a legal entity before establishing the business relationship or carrying out the transaction, in their physical presence unless otherwise laid down by the Act. Therefore, it is concluded that in the cases where CDD is obligatory financial institutions are required to identify the customer (natural or legal person, a person represented by virtue of authorisation and the representative) and to verify that customer's identity.

336. Sections 7 and 8 of the AML/CFT Act elaborate, for the purpose of this Act, the concepts of "identification" and "verification of identification" respectively. According to Section 7 identification for natural persons means identifying a natural person's name, surname and birth registration number or date of birth, his address of permanent residence or other residence, nationality, type and number of his identification document. For a natural person being an entrepreneur identification is understood also as identification of his place of business, business identification number, if allocated, designation of the official register or other official record in which the entrepreneur is entered and the number of registration into that register or record.

337. For the purposes of the AML/CFT Act, verification of identity is understood as verification of the data in his identification document if contained therein and verification of the appearance of the person by comparing it to the appearance on his identification document in his physical presence. (Section 8 of the AML/CFT Act).

338. Besides, according to paragraphs 1 and 2 of Article 89 of the Act on Banks, each client (natural or legal person) has to be identified in respect of transactions. In relation to natural persons, the Act on Banks states that identity may be verified by a "document of identity" or by his signature if he is known in person and the signature matches the specimen signature kept in the bank. In the insurance and securities sectors there are requirements for verification by documents of identity. But unlike the Act on Banks there is no clear definition of what should amount to reliable documents of identity. The representatives of these sectors interviewed during the on-site visit indicated that they, in practice, follow the approach taken in the Act on Banks (verification based on the identity card or equivalent). Slovak legislation, such as the Act No. 224/2006 Coll. on identity card (including amendments to certain acts), as amended; the Act No. 647/2007 Coll. on travel documents, as amended; the Act No. 48/2002 Coll. on the stay of foreigners (including amendments to certain acts), as amended and Act No. 480/2002 Coll. on asylum (including amendments to certain acts), as amended, specify which documents may be used for the purpose of identification of a natural person.

Identification of legal persons or other arrangements (c.5.4)

339. Section 7 (b) of the AML/CFT Act states that identification of legal persons means to identify the legal entity's business name, address of registered office, identification number, designation of

the official register or other official record in which the legal entity is entered and the number of registration into that register or record and identification of a natural person who is authorised to act on behalf of the legal entity. According to Section 8 (b) of the AML/CFT Act, verification in the case of a legal entity means to corroborate the data on the basis of documents, data or information obtained from the official register or other official record in which the legal entity is entered or from other reliable and independent source and verification of the identity of a natural person who is authorised to act on behalf of the legal entity to the extent of the data in his physical presence and verification of the power to act on behalf of the legal entity.

340. In the case of a person represented by virtue of authorisation, according to Section 7 (c) of the AML/CFT Act, identification means to identify his data (as a natural or legal person) and to identify the data of a natural person authorised to act on behalf of that legal entity or natural person (as a natural person). Section 8 (c) of the AML/CFT Act requires obliged entities to verify his data to the extent of data on the basis of documents, data or information obtained from the submitted authorisation containing an authenticated signature, from the official register or other official record or from other reliable and independent source and verification of identification of a natural person who is authorised to act on the basis of authorisation to the extent under Section 7 (a), in his identification document in his physical presence.

341. Furthermore, in the case of banks, more detail is generally provided on the identification and verification process in the Act on Banks. Article 93a of this Act requires banks to verify the authorisation of the representation where the proxy is involved.

342. All of these issues have also been developed in the Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing. The document stresses the duty to find out whether the customer is acting on his own behalf. For the purposes of the Methodological guidance, it is necessary to understand the "performance of a transaction on one's own expense" or "with one's own funds" as action on one's own behalf. Pursuant to Section 10 (10) of the AML/CFT Act, it is necessary to find out this fact always in situations stated in Article 10 (2) of the AML/CFT Act and in accordance with Article 89 (3) of the Act on Banks, even if the transaction is a transaction of at least €15,000 (i.e. not only a "casual" transaction, as the Act implies). The detection and, to an adequate extent, also the verification of the beneficial owner primarily follows the provisions of Articles 9 and 10 of the Act, with the Act on Banks also partially dealing with this important element of the basic and enhanced customer diligence in Article 93a.

The identification of the beneficial owner (c. 5.5)

343. According to paragraph 1 (b) of Section 10 of the AML/CFT Act all obliged entities should identify the beneficial owner and take adequate measures to verify his identification, including measures to determine the ownership structure and management structure of a customer being a legal entity or a corporation. Furthermore, paragraph 10 of the same Article requires obliged entities to determine when carrying out CDD whether the customer acts in his own name. If it transpires that the customer does not act in his own name, the obliged entity should ask the customer to submit a binding written statement to prove name, surname, birth registration number or date of birth of a natural person or business name, registered office and identification number of a legal entity on whose behalf the transaction is being carried out. The obliged entity should follow the same procedure also in case if there are doubts whether the customer acts in his own name. Some sectoral laws contain similar provisions. Article 89, paragraph 3, in relation with Article 93 a) of the Act on Banks require the determination of whether the customer acts on his own behalf and the taking of reasonable steps to verify the identity of that other person. Paragraph 5 of Article 73 of the Securities Act states the obligation of identification only for transactions over €15,000. Finally,

Article 13, paragraph 5, letter c) of Foreign Exchange Act contains a cross reference to obligation stated in the AML/CFT Act to each transaction in foreign exchange assets. The Evaluation team assumes that this provision refers to the FATF requirement to determine whether a customer is acting on behalf of another person.

344. The Slovak AML/CFT Act contains no further obligation for financial institutions to take reasonable measures to verify the identity of the beneficial owner using relevant information or data obtained from a reliable source such that the financial institution is satisfied that it knows who the beneficial owner is. According to the Methodological Guidance of the Financial Market Supervision Unit of the National Bank of Slovakia of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing (page 14), which is not other enforceable means, the "verification of the acquired information on the beneficial owner in accordance with the Act is supposed to be carried out to an adequate extent; e.g. by requesting a written declaration on the beneficial owner and subsequent verification of such information from available sources". However, as criterion 5.5 is an asterisked one such an obligation should be introduced in law or regulation through a comprehensive provision covering reasonable measures to be taken by financial institutions in order to verify the identity of the beneficial owner.

345. Section 9 (b) of the AML/CFT Act defines the beneficial owner as *"a natural person for the benefit of whom a transaction is being carried out or a natural person who*

1. *has a direct or indirect interest or their total at least 25 % in the equity capital or in voting rights in a customer being a legal entity - entrepreneur including bearer shares, unless that legal entity is an issuer of securities admitted to trading on a regulated market which is subject to disclosure requirements under a special regulation,*
2. *is entitled to appoint, otherwise constitute or recall a statutory body, majority of members of a statutory body, majority of supervisory board members or other executive body, supervisory body or auditing body of a customer being a legal entity –entrepreneur,*
3. *in a manner other than those referred to in subsections 1 and 2 controls a customer being a legal entity –entrepreneur,*
4. *is a founder, a statutory body, a member of a statutory body or other executive body, supervisory body or auditing body of a customer being a corporation or is entitled to appoint, otherwise constitute or recall those bodies,*
5. *is a beneficiary of at least 25% of funds supplied by a corporation, provided the future beneficiaries of those funds are designated or*
6. *ranks among those persons for whose benefit a corporation is established or operates, unless the future beneficiaries of funds of the corporation are designated".*

346. In respect of determination of natural persons that ultimately own or control the customer (criterion 5.5.2 (b)), there's no further provision in the Slovak AML-CFT framework. Apart from the referred Section 10 (10) AML Act, there's no specific requirement for companies to identify natural persons with a controlling interest and natural persons who comprise the decision-making and management authority of a company.

Information on purpose and nature of business relationship (c.5.6)

347. Financial institutions are required to obtain information on the purpose and intended nature of the business relationship (Section 10, paragraph 1 (c) of the AML/CFT Act).

Ongoing due diligence on business relationship (c.5.7, 5.7.1 & 5.7.2)*

348. The obligations to conduct ongoing monitoring of the business relationship and to keep documents, data and information collected under the CDD process up-to-date are covered in

paragraph 1 (d) of Section 10 of the AML/CFT Act fully in line with essential criteria 5.7, 5.7.1 and 5.7.2 almost verbatim. The ongoing monitoring of the business relationships is explained at length in the Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing. Furthermore, paragraph 8 of the same section requires obliged entities to verify, depending on the risk of ML and TF, the validity and completeness of identification data and information collected under the CDD process also during the business relationship and to record their changes.

Risk – enhanced due diligence for higher risk customers (c.5.8)

349. As noted above, the CDD measures are applied on a risk sensitive basis. According to paragraph of Section 10 of the AML/CFT Act obliged entities shall determine the extent of CDD in proportion to the risk of ML and TF. The risk of ML or TF for the purposes of this Act shall be considered by the obliged entity with regard to the customer, type of transaction, business relationship or a particular transaction.

350. The AML/CFT Act requires obliged entities to perform enhanced due diligence if, according to the information available, some of the customers, some types of transactions or some particular transactions represent a higher risk of ML or TF. In the case of enhanced due diligence, obliged entities are required to perform, in addition to normal CDD measures, further measures depending on the ML or TF risk (Section 12 (1) of the AML/CFT Act). Enhanced customer due diligence is required in any case for non face-to-face business relationships, cross-border correspondent banking relationships with a credit institutions of non-EU Member State and PEPs. Those three enhanced risk-categories are modelled on the risk-based approach set out in the Third EU AML/CFT Directive. Section 12 of the AML/CFT Act describes the types of additional measures required to be applied (see detail under Recommendations 6 and 7 below). It appears that it is up to the financial institution to decide what type of further measures are adequate in other situations that they identified as posing higher risk.

Risk – application of simplified/reduced CDD measures when appropriate (c.5.9)

351. Financial institutions can also apply reduced measures (criterion 5.9) in certain cases. The possibility to apply simplified due diligence is covered in Section 11 of the AML/CFT Act dealing with Simplified Due Diligence that reads:

"Obliged entity shall not be obliged to perform customer due diligence

a) if the customer is a credit institution or a financial institution under Section 5 subsection 1, letter b) of point 1 to 10 which operates in the territory of a EU Member State or other state party to the European Economic Area Treaty (thereinafter referred to as "Member State"),

b) if the customer is a credit institution or a financial institution which operates in the territory of a third country which imposes them obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by this Act and with regard to performance of those duties they are supervised,

c) if the customer is a legal entity whose securities are negotiable on a regulated market in a Member State or is a company which operates in the territory of a third country which imposes them obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by this Act and being subject to disclosure requirements equivalent to requirements those under a special regulation,[37])

d) to the extent of identification and verification of identification of the beneficial owner if a pooled account is managed by a notary or an advocate who operates in the Member State or in a third country which imposes obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by this Act and if the data on identification of the beneficial owner are available, on request, to the obliged entity that keeps this account,

e) if the customer is a Slovak public authority,
f) if the customer is a public authority and if
1. *it has been entrusted with public functions under the European Union Treaty, under agreements of the European communities or secondary legal acts of the European communities,*
2. *its identification data are publicly available, transparent and there are no doubts about their correctness,*
3. *its activity is transparent,*
4. *its bookkeeping provides an accurate and true view of the subject of bookkeeping and its financial standing and*
5. *it accounts to a European community's institution or a Member State authority or there exist other appropriate procedures which ensure control of its activity.*

(2) Obliged entity shall not be obliged to perform customer due diligence upon

a) life insurance policy if the premium in the calendar year is no more than €1,000 or the single premium is no more than €2,500,
b) a policy for retirement pension insurance with a pension asset management company entered in the retirement pension insurance policies register,[8])
c) supplementary pension savings,
d) electronic money under a special regulation,[9]) if the maximum amount stored in the electronic payment device which is impossible to recharge shall not exceed €150, if the total amount of transaction shall not exceed €2,500 in the calendar year concerning the electronic payment device which is possible to recharge except the case if the bearer converts an amount higher than €1,000 in the same calendar year or
e) types of transaction posing a low risk of being exploited for legalisation or terrorist financing and meeting the following conditions:
1. *contract on provision of the type of transaction is in writing,*
2. *payments within the type of transaction are carried out solely via an account held on the customer's name in a credit institution in a Member State or a third country which performs measures in the area of the prevention and detection of legalisation and terrorist financing equivalent to measures laid down by this Act,*
3. *neither the type of transaction nor payments within the scope of the type of transaction are not anonymous and their nature enables detection of an unusual transaction,*
4. *a maximum limit of amount of €15,000 is determined for the type of transaction,*
5. *proceeds of the transaction cannot be carried out for the benefit of a third party, except cases of death, disability, the attainment of a pre-determined age or other similar event,*
6. *where concerning the types of transaction which allow for investments into financial assets or receivables including insurance or other type of contingent receivables, proceeds may be realised only in the long time period, the type of transaction cannot be used as a guarantee, the type of transaction does not enable express payments and the business relationship cannot be rescinded or terminated prematurely.*

352. Section 11 reflects the derogation in the Third EU AML/CFT Directive. This derogation departs from the FATF Recommendations, which require the application of reduced or simplified measures, rather than exemptions. The Slovak Republic does not apply any exemptions from AML/CFT requirements where there is any ML risk.

[8] Section 2 of Act 43/2004 Coll. as amended

[9] Section 21 of Act 510/2002 Coll. as amended

Risk – simplification/ reduction of CDD measures relating to overseas residents (c.5.10)

353. As regards non-resident clients the reduced diligence applicable to identification applies for all credit and financial institutions as referred in Section 11, paragraph 1 (a) and (b) AML/CFT Act.

(1) Obliged entity shall not be obliged to perform customer due diligence
a)if the customer is a credit institution or a financial institution under Section 5 subsection 1, letter b) of point 1 to 10 which operates in the territory of a EU Member State or other state party to the European Economic Area Treaty (thereinafter referred to as "Member State"),
b)if the customer is a credit institution or a financial institution which operates in the territory of a third country which imposes them obligations in the area of the prevention and detection of legalisation and terrorist financing equivalent to obligations laid down by this Act and with regard to performance of those duties they are supervised.

354. Nevertheless, as stated in the Methodological Guidance (Part E), having a client from a Third Equivalent Country does not automatically mean exemption form the obligation to monitor the business relationship, to detect unusual transactions or to report them including the obligation to keep all customer's documents.

355. In order to inform about the level of compliance to international standards in concrete countries, the FIU web site provides and updates both the list of Third Equivalent Countries as elaborated under the umbrella of the CPLMLTF and all FATF and MONEYVAL Public Statements,

Risk – simplified/reduced CDD measures not to apply when suspicions of ML/FT or other risk scenarios exist (c.5.11)

356. Paragraph (3) of Section 11 of the AML/CFT Act clearly stipulates that CDD has to be performed if there is a suspicion that the customer is preparing or carrying out an unusual transaction and in doubts whether it is the case of simplified due diligence.

Risk-based application of CDD to be consistent with guidelines (c.5.12)

357. According to Section 20 of the AML/CFT Act, obliged entities are required to prepare their own activity programmes that should contain, inter alia, the way of performing CDD and the method of risk assessment and risk management under Section 10 (4).

358. The Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia, No. 4/2009, for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing develops a risk-based application of CDD issues. However, apart from this guidance addressed to the banks, no such guidelines for the rest of the obliged entities have yet been issued by the authorities.

359. In addition, there is no legal requirement in Slovak legislation which requires that the determination of the extent of the CDD measures on a risk sensitive basis should be consistent with guidelines issued by the competent authorities.

Timing of verification of identity – general rule (c.5.13) (c.5.14 & 5.14.1)

360. Except for the cases described below obliged entities are required to verify the identity of the customer being a natural person and the identity of each person acting on behalf of the customer being a legal entity before establishing a business relationship or carrying out a transaction, in their physical presence unless otherwise laid down by this Act. (paragraph 6 of Section 10 of the AML/CFT Act)

361. Paragraph 7 of Section 10 of the AML/CFT Act, however, provides that an obliged entity may complete the verification of the customer's or beneficial owner's identification during the establishment of a business relationship if this is necessary not to interrupt the common conduct of business and where there is a low risk of ML or TF. Nevertheless, in such cases, the obliged entity should complete the verification without delay after the customer is physically present for the first time at the obliged entity.

362. According to the referred article the completion of the identification process can not be delayed or postponed, so the consideration of criterion 5.14.1 is, in principle, inappropriate in the Slovak context.

Failure to satisfactorily complete CDD before commencing the business relationship (c.5.15) and after commencing the business relationship (c.5.16)

363. Section 15 of the AML/CFT Act obligates the obliged entities to refuse to establish a business relationship or to carry out a particular transaction, or to terminate a business relationship where:
- obliged entities may not perform CDD for reasons on the part of the customer or
- the customer refuses to prove on whose behalf he acts.

364. In addition, obliged entities are required without undue delay to report to the FIU the refusal to carry out the unusual transaction under Section 15.

Existing customers – (c.5.17 & 5.18)

365. Concerning the requirement to perform full CDD on existing customers this is included set out in paragraph 1 of Section 36 of the AML/CFT Act. This section reads: *"Obliged entity shall perform customer due diligence under Section 10 and enhanced due diligence under Section 12 also in relation to the existing customers depending on the risk of legalisation or terrorist financing by 31 December 2009."* Furthermore, as set out above, Section 10 of the AML/CFT Act require ongoing monitoring of the business relationship and the keeping of documents, data and information collected under the CDD process up-to-date.

366. In practice, the NBS during its inspections checks whether old customers have been identified and their identities have been verified according to the AML/CFT Act.

Effectiveness and efficiency

367. Customers due diligence measures for financial institutions are legally covered. The AML/CFT Act broadly sets out major preventive standards for obliged entities. Besides, in the case of banks, the "Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing" contributes to clarifying how to implement CDD issues.

368. As far as banks are concerned, the evaluation team has been convinced that the implementation of R.5 in Slovakia is quite effective as they have developed a comprehensive preventive regime. However, some deficiencies in the implementation of CDD measures appear to have been detected during the FIU and the NBS inspections, but their gravity is not that significant.

369. Concerning the rest of the financial institutions, most of them seemed to have a good understanding of international AML standards. Nevertheless, some of them (such as securities pension funds and payment services), appear not to be aware of the ML risks that threat their

sectors. Slovak authorities should issue specific methodological guidelines for each sector in order to improve general performance of CDD measures.

Recommendation 6 (rated NC in the 3rd round MER)

Risk management systems, senior management approval, requirement to determine source of wealth and funds and on-going monitoring (c. 6.1- c. 6.4)

370. Recommendation 6 was rated as *"Non-Compliant"* in the 3rd round evaluation and it was commented that Slovakia did not implement measures on enhanced due diligence in relation to PEPs.

371. The new AML/CFT Act has introduced the concept of PEPs into the Slovak law. The Act now provides for the definition of politically exposed person as natural person who is entrusted with a prominent public function and not having permanent residence in the Slovak Republic during performance of his function and until one year after the termination of performance of a prominent public office. The said wording of the AML/CFT Act indicates that persons holding prominent public functions but residing permanently in the Slovak Republic are not being recognised as PEP under this definition. Although this definition follows the provisions of the Third EU AML/CFT Directive, the FATF definition relates directly not to the place of residence of a person in question but to the fact that he/she has been entrusted with prominent public functions in a foreign country. However, according to the Act No 253/1998 on the Reporting of Residence of the Slovak Republic Citizens and on the Register of Slovak Inhabitants a permanent residence can only be granted to a Slovak citizen. Notwithstanding this fact, the definition of PEPs in the Slovak law still does not apply to any Slovak citizen who has been entrusted with a prominent public function abroad, but has a permanent residence in the Slovak Republic, which might indeed be possible.

372. The PEPs, according to second paragraph of Section 6, include the following categories:

- *head of state, prime minister, deputy prime minister, minister, head of a government agency, state secretary or a similar deputy of a minister,*
- *member of Parliament,*
- *judge of the supreme court, judge of the constitutional court or other high-level judicial bodies the decisions of which are not subject to further appeal, except for special cases,*
- *member of the court of auditors or of the central bank board,*
- *ambassador, chargé d'affaires,*
- *high-rank military officer,*
- *member of executive body, supervisory body or auditing body of a state enterprise or a state-owned company or*
- *a person holding a similar post in the institutions of the European Union or international organisations.*

373. The definition of PEPs follows the definition of the Third EU AML/CFT Directive and the Implementation Directive (Article 31, paragraph 2). Nonetheless, it is not fully in line with the PEP definition provided in the Glossary to the FATF Recommendations, as it does not fully cover senior politicians, senior government officials (for example non-political heads of ministries) and important party officials. This is because the definition provided in the Third EU AML/CFT Directive was transposed into Slovak law (Section 6 (2) of the AML/CFT Act) in a way, which provides a closed catalogue of PEPs. The actual wording ("shall mean") does not allow the conclusion that people referred to as "entrusted with prominent public function", but not directly mentioned in this section, can also fall under this definition.

374. The AML/CFT Act subjects any transactions with PEPs to enhanced CDD measures.

375. According to paragraph 11 of Section 10 of the AML/CFT Act, depending on the ML and TF risk, all obliged entities including financial institutions are obliged to take measures to determine whether the customer is a PEP. This provision, however, does not provide for a direct obligation to determine if the beneficial owner of a client is a PEP. This is also true for the Methodological guidance, which does not address this issue at all (see, page 15 of the said document).

376. Each time a client is identified as a PEP, the obliged entity must apply enhanced customer due diligence measures (Section 12(c) of the AML/CFT Act). One of those measures is obtaining approval from a senior management member before establishing a business relationship.

377. It is also important to stress that enhanced due diligence comprises an obligation to detect the origin of property and origin of funds of the client.

378. The said business relationship with PEPs is subject to scrutiny and detailed monitoring.

379. It is, however, also essential for the country to introduce the obligation to require financial institutions to obtain senior management approval to continue the business relationship with a client, should he be subsequently found to be a PEP. There is no such obligation whatsoever in the Slovak law.

Additional elements

Domestic PEP-s – Requirements

380. At the time of the on-site visit there was no provision in the Slovak law, which required financial institutions to extend the requirements of enhanced due diligence to clients who hold prominent public functions domestically.

381. As the evaluation team was advised, despite not having this provision in the Slovak law, upon application of risk-based approach within customer due diligence, the obliged entities reported the following number of domestic politically exposed persons: 2009 – 6 reports, 2010 – 10 reports. The reports in the above mentioned cases were reported to the Slovak FIU fully in compliance with AML/CFT Act as far as the transactions involved were considered by obliged entities as unusual and the clients to be risky upon application of risk-based approach.

Ratification of the Merida Convention

382. The National Council (Parliament) of the Slovak Republic adopted the UN Convention against Corruption (the Merida Convention) by its Resolution no. 2145 dated on 15 March 2006 and the President of the Republic ratified it on 25 April 2006. The Convention is in effect on the territory of the Republic of Slovakia since 1 July 2006. As the evaluation team was advised the UNCAC was implemented, *inter alia*, in the new Criminal Code and Criminal Procedure Code and by the Act no. 224/2010 Coll. which introduced the corporate liability. The implementation of the UNCAC in the Slovak Republic is currently under the review of the Implementation Review Group (IRG).

Effectiveness and efficiency

383. The interviews with the private sector representatives during the on-site visit revealed that the financial institutions are generally very much aware of their obligations arising form the AML/CFT Act.

384. Financial institutions follow all obligations relating to PEPs, as specified by the Act and compliance policies of their major shareholders, being the international financial groups. Commercial databases are in common use, and the screening process also includes UBO's, which as mentioned above, is not a requirement of the law.

385. The Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia of 17 December 2009 No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing can be also indicated as a mean to ensure effectiveness, by providing the financial sector with clarification on issues arising form the legislation.

386. The evaluation team is convinced as to the fact that the implementation of R.6 in Slovakia is effective, as far as the financial institutions are concerned.

Recommendation 7 (rated NC in the 3rd round MER)

Require to obtain information on respondent institution & Assessment of AML/CFT controls in Respondent institutions (c. 7.1 & 67.2)

387. Criteria 7.1 to 7.4 cover cross border banking and other similar relationships. The AML/CFT Act in paragraph 2 (b) of Section 12 implements the said criteria in line with the Third EU AML/CFT Directive, providing for a sufficient regulatory framework in this matter. Each time a cross-border relationship is to be established with a credit institution of a non-EU Member State it is to be treated as a factor triggering enhanced due diligence measures.

388. According to point 1 in letter (b) of the mentioned section, the obliged entities (including financial institutions) are obliged to collect information from publicly available sources about a respondent credit institution to determine the nature of its business, its reputation and efficiency of supervision. This can be done from publicly available information.

389. The obliged entities also have to assess the control mechanisms of the respondent credit institution in the AML/CFT area, and ascertain the respondent credit institution's authorisations to perform its activities, as stated in points (2) and (4) of the mentioned section.

Approval of establishing correspondent relationships (c.7.3)

390. Each correspondent banking relationship must have a prior approval given by a senior management member. (paragraph 2, b (3) of Section 12 of the AML/CFT Act)

Documentation of AML/CFT responsibilities for each institution (c.7.4)

391. Criterion 7.4 requires the financial institutions to document the respective AML/CFT responsibilities of each institution on the cross-border correspondent banking relationship. The evaluation team was advised by the financial sector representatives during the on-site visit that it is done by the nature of an agreement concluded in written form. It is however important to state that this particular obligation arising from criterion 7.4 is not present in any law, regulation or other enforceable means in the Slovak law. The evaluation team is convinced however by the interview with the private sector representatives on-site that the practice in respect of correspondent banking relations is in line with criterion 7.4 even though this particular stipulation is not copied explicitly in the Slovak legislation. Nevertheless, the Slovak authorities should therefore consider amending the AML/CFT Act to include to practice already existing in the financial market as it allows for the full compliance with the FATF standard.

Payable through Accounts (c.7.5)

392. In respect of payable through accounts, the obliged institutions must be satisfied that a respondent credit institution has verified the identification of a customer and performed customer due diligence on the customer having a direct access to the respondent credit institution's account and that the respondent credit institution is able to provide relevant customer due diligence data upon request.

393. The assessors have noted that paragraph 2 letter b of Section 12 of the AML/CFT Act relates directly to cross-border correspondent relationship with non-EU Member States. Literal interpretation of this provision causes it to fall short of the FATF standard, which recognises correspondent banking as a high risk situation. Recommendation 7 does not also provide for any concessions. It can be argued, and not without reason, that the FATF's recognition of the EU as a single jurisdiction can be applied to this situation as well. It is, however, a belief of the evaluators that the FATF's recognition in relation to SR.VII and IX cannot simply be transferred to Recommendation 7, and must be sought and achieved by the EU to this recommendation alone.

Effectiveness and efficiency

394. It is concluded that with the adoption of the new AML/CFT Act, Slovakia has now sufficient regulatory framework which remedies the deficiencies identified in the 3rd round MER in relation to R.7.

395. As mentioned above, the financial institutions are generally very much aware of their obligations arising form the AML/CFT Act. The obligations in respect of cross-border correspondent banking relationship are being observed by financial institutions. Due care is placed on such relationships if the respondent institution is not a financial institutions from the EU or an equivalent third country.

396. No issues impeding in any way the evaluation of effectiveness of implementation of R.7 have been made known to the evaluation team.

Recommendation 8 (rated NC in the 3rd round MER)

Misuse of new technology for ML/FT (c.8.1)

397. Due to the absence of any specific enforceable guidance on measures to be put in place to avoid the risks associated with technological developments and non-face to face relationships, Recommendation 8 was rated "Non-Compliant" in the 3rd round MER. The AML/CFT Act now contains basic general requirements. Under paragraph 2 (b) of Section 14 of the AML/CFT Act, dealing with "Detection of an Unusual Transaction", financial entities are obliged to pay special attention, "*to any risk of legalisation or terrorist financing that may arise from a type of transaction, a particular transaction or new technological procedures while carrying out transactions that may support anonymity and is obliged to take appropriate measures, if needed to prevent their use for the purposes of legalisation and terrorist financing*". Moreover, according to paragraph 2 of Section 24 of the AML/CFT Act, financial institutions are prohibited from entering into a business relationship or from performing any transaction on an anonymous basis.

398. The Slovak authorities and the sectors' representatives interviewed advised that other than the relevant provisions in the AML/CFT Act, there is no specific guidance regarding new technological developments and the need for internal policies within financial institutions to prevent the misuse of technological developments in ML or TF.

399. Thus, these issues should be resolved within the obliged entities. In practice, banks apply special security measures ("electronic signature certificate" or PIN code, numbered passwords) when providing services through online or telephone banking.

400. The Slovak authorities advised the evaluation team that there were no other new payment methods used in Slovakia.

Risk of non-face-to-face business relationships (c8.2)

401. Concerning non-face to face business, the AML/CFT Act states the obligation for enhanced CDD measures. In particular, paragraph 6 of Section 10 of the AML/CFT Act defines a duty for all the reporting entities to verify identity of the customer being a natural person and identification of each person acting on behalf of the customer being a legal entity before establishing the business relationship or carrying out the transaction, in their physical presence. If this condition is not met the reporting entities are obliged to carry out enhanced due diligence in line with paragraph 2 (a) of Section 12 of the AML/CFT Act.

402. In practice, as evaluation team was told in interviews held during the on-site visit, direct contact with the customer still remains the fundamental rule in the opening of an account (credit institutions), establishing a business relationship or executing a transaction (financial institutions).

Effectiveness and efficiency

403. As mentioned above, Slovakia has a general legal framework in place concerning new technologies and non-face to face business relationships.

404. However, effective compliance is difficult to be averred. The FIU representatives interviewed about their on-site procedures on this obligation explained that some problems where found in a concrete financial institution but affirmed that these had already been solved.

405. No specific guidance on new technologies and non-face to face business relationships has been issued as yet. It would be useful if the Slovak Authorities did adopt such a document in order to develop how CDD measures should operate in non-face to face transactions.

3.2.2 Recommendations and comments

Recommendation 5

406. With the adoption of the new AML/CFT Act, Slovakia rectified all of the deficiencies identified in the 3rd round MER in relation to customer due diligence measures. However, further legislative clarifications are still needed for the full compliance with the FATF standards. The Slovak authorities should introduce a more comprehensive provision regarding reasonable measures to be taken by financial institutions in order to verify the identity of the beneficial owner. In addition, they should review the identification process in respect of low risk customers/circumstances/businesses to one of reduced or simplified customer due diligence instead of granting exemptions.

407. The Slovak authorities should issue guidance for some sectors such as securities, pension funds and payment services to make them aware of sectoral AML/CFT risks

Recommendation 6

408. The Slovak authorities are encouraged to review the definition of PEP to fully reflect the one provided in the Glossary to the FATF Recommendations. In particular, it should cover senior politicians, senior government officials (for example non-political heads of ministries) and important party officials.

409. Although the AML/CFT Act obliges to undertake enhanced due diligence measures when establishing a business relationship with a PEP, there is no specific requirement to find out whether the beneficial owner of the contracting party might be a PEP. The Slovak authorities should consider addressing this issue either in law or regulation or other enforceable means.

410. As the FATF standard should be applicable to persons entrusted with prominent public functions in a foreign country, it is advisable not to limit the provisions of Slovak law only to foreign PEPs residing abroad.

411. There is no provision for senior management approval to continue the business relationship where the customer subsequently is found to be or becomes a PEP, which falls short of the FATF standard. The Slovak authorities should cover this obligation by law, regulation or other enforceable means.

Recommendation 7

412. The Slovak authorities should consider providing in law, regulation or other enforceable means an obligation for financial institutions to document the respective AML/CFT responsibilities of each institution on the cross-border correspondent banking relationship, for both EU and non-EU correspondent relationships.

413. The Slovak authorities should extend the enhanced CDD measures to respondent banks within the EU.

Recommendation 8

414. The Slovak Republic was involved in several cases where organised groups (from Romania) abused internet services and offered different goods for sale. Thus, crimes like internet fraud, phishing or pharming are real risks to citizens in Slovakia.

415. Therefore, specific guidance regarding new technological risks and the need for internal policies within financial institutions to prevent the misuse of technological developments in money laundering or financing of terrorism need to be issued.

3.2.3 Compliance with Recommendations 5, 6, 7 and 8

	Rating	Summary of factors underlying rating
R.5	**LC**	• Lack of specific guidelines for each financial sector apart from the banking sector for improving general performance of CDD measures. • Lack of sufficiently comprehensive provision regarding reasonable measures to be taken by financial institutions in order to verify the identity of the beneficial owner.

		• Certain categories of low risk business can be exempted from CDD instead of requiring simplified or reduced measures. • Lack of awareness in some sectors such as securities, pension funds and payment services about the AML/CFT risks.
R.6	**PC**	• No provision to verify if the beneficial owner is PEP in the Slovak Law is present. • Provisions do not apply to foreign PEPs residing in Slovakia. • The definition of PEPs is not sufficiently broad to include all categories of senior government officials. • No provision for senior management approval to continue business relationship where the customer subsequently is found to be or becomes PEP.
R.7	**LC**	• No enforceable requirement to document the respective AML/CFT responsibilities of each institution. • Special measures apply only to non-EU correspondent relationships.
R.8	**PC**	• Effective compliance is not demonstrated. • Lack of guidance concerning new technologies risks and on how CDD measures should operate in non- face to face transactions.

3.3 Financial institution secrecy or confidentiality (R.4)

3.3.1 Description and analysis

Recommendation 4 (rated LC in the 3rd round MER)

416. This area is regulated by Article 91 of the Act on Banks. Article 91(4) of that Act provides that client information that would otherwise be subject to bank secrecy may be disclosed under a number of circumstances, including a request in writing by a law enforcement or regulatory authority. In addition, reporting unusual transactions and reports of suspicious activities are not regarded as breaches of banking secrecy under article 91(7) of the Act on Banks. Paragraph 6 of Section 7 of the AML/CFT Act provides that fulfilment of obligations under the AML/CFT Act will not constitute a violation of the professional secrecy for any obliged entity. As noted in the 3rd round MER, there are no reported practical restrictions in the Slovak legislative framework limiting competent authorities from performing their anti-money laundering functions. The FIU is able to access further information from reporting entities in analysing reports. The evaluators received the impression that this criterion is still adequately met.

417. Information is shared between competent authorities based on Memoranda of Understanding. Certain deficiencies were noted in this regard in the 3rd round MER, particularly regarding exchange of information between domestic prudential supervisory authorities. Since that point, the Slovak authorities have advised that the National Bank Services now serves as the single supervisory authority over the financial sector. Taking into account the amendments to the AML/CFT Act in force since September 2008, the evaluators received the impression that the deficiencies noted in the 3rd round MER had been remedied and that there is no impediment to sharing information between competent authorities when appropriate.

Effectiveness and efficiency

418. The evaluation team found no indication that the exchange of information is in any way hindered in practice.

3.3.2 Recommendations and comments

419. This Recommendation is fully observed, and, the evaluation team, therefore, has no recommendations.

3.3.3 Compliance with Recommendation 4

	Rating	Summary of factors underlying rating
R.4	**C**	

3.4 Record Keeping and Wire Transfer Rules (R.10 and SR. VII)

3.4.1 Description and analysis

Recommendation 10 (rated LC in the 3rd round MER)

420. Although Recommendation 10 was rated *"Largely Compliant"* in the 3rd round MER it needs to be reassessed in accordance with the requirements of mutual evaluation procedure for this assessment round.

Record keeping & reconstruction of transaction records (c.10.1 and 10.1.1)

421. The basic record-keeping obligations are regulated under Section 19 of the AML/CFT Act. Pursuant to paragraphs 1 and 2 of this section, all obliged entities are required to keep data or written documents obtained from the customer during the application of CDD and enhanced due diligence measures for a period of five years after the business relationship with the customer is ended. Similarly obliged entities are obliged to maintain all data and written documents about the transaction for a period of five years from the moment of the carrying out the transaction. According to third paragraph of Section 19, obliged entities are required to keep such data and written documents for a longer period if the FIU requests to do so. In that case, the FIU shall specify in written form the period and scope of keeping data and written documents. However, it is important to note that only the FIU, for its own purposes or upon request from another Unit within the Police Force, can request all obliged entities to keep records for a longer period. The NBS can ask for the prolongation of the record-keeping period in its supervisory activities in the cases stated in paragraph 3 of Article 75 of the Securities Act and paragraph 4 of Article 36 of the Act on Financial Intermediation and Financial Counselling. Law enforcement authorities and prosecutors, however, do not have such a power. Moreover, it must be considered that in case of investigation of economic crimes all records can be seized for the purpose of criminal evidence and expertise so that it be possible to permit both reconstruction of individual transactions and linked transactions in the investigated case. The legal obligation of law enforcement authorities is to ensure that evidence enters into criminal proceedings without delay to prevent its destruction or damage.

422. Under essential criterion 10.1*, obliged entities are required to maintain all necessary records on transactions, both domestic and international, for at least five years following the completion of transactions. Furthermore, transaction records should be sufficient to permit reconstruction of individual transactions. This provision is broadly covered under Section 19, para 2 (a) and (b), which must be applied by all obliged entities. Besides, in order to clarify the scope of "all data and written documents" necessary to be kept by obliged entities, the Slovak FIU has elaborated some "Guidelines" that are published on the Slovak FIU's website Given the broad language used in paragraph 2 (b) of Section 19 of the AML/CFT Act which requires keeping of "all data and written documents", and the definition of "transaction" under Section 9 (h) of the same act, it can be interpreted that the Act covers the requirements of criterion 10.1*.

423. To ensure that the scope of transaction records kept is sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity (as required under essential criterion 10.1.1), several Acts contain specific requirements for financial institutions. The AML/CFT Act does not contain any explicit requirement about the scope of the transactions records to be kept. However, Article 2, paragraph 7 of the Act on Supervision of the Financial Market states a general provision as follows:

> *"A supervised entity, members of its bodies, its employees and other persons, whose activities are related to the supervised entity, shall be obliged to enable the performance of supervision, refrain from any action that could frustrate the performance of such supervision, and provide, in the state language, any information, documentation, concurrence and assistance required by the National Bank of Slovakia or supervising officers for the purposes of performing supervision (…)"*

424. In particular, for banks or branch offices of foreign banks the Article 42, paragraph 1, Article 89 and Article 93 a) of the Act on Banks state the obligation of maintaining of transactions records and the scope of the information that must be kept as follows: *"Banks, foreign banks and branch offices of foreign banks are obligated to store the copies of documents and protect them against damage, alteration, liquidation, loss, theft, disclosing, misusing and unauthorised access and the copies of documents and data on verification of client identity, documents determining ownership of money used by clients to conduct transactions, and documents on conducted operations for at least five years after a transaction, contract, etc. is concluded"*. The Securities Act, in its Article 73, paragraph 6 contains a particular provision regarding the obligation of record-keeping for stock brokerage firms and foreign stock brokerage firms in their operations in the territory of the Slovak Republic for at least ten years as follows: *"The stock brokerage firm and the foreign stock brokerage firm shall retain and protect the data against damage, alteration, liquidation, loss, theft, disclosure, misusage and unauthorised access and copies of client identification and of documents identifying the owner of the funds used by the client to accomplish the trade and contracts, and other documents on deals made for at least ten years from conclusion of the transaction"*. According to Article 21, paragraph 5 of the Act on Collective Investment, management companies should *"for at least ten years after concluding a transaction store identification information and copies of documents proving the identity of investors and customers and documents confirming the ownership of funds used by investors and customers to make the transaction"* The Act on Insurance (Article 47, paragraph 9) states as follows: *"The insurance company, branch of an insurance company from another Member State and branch of a foreign insurance company shall be obliged to maintain and protect the insurance contracts including changes and related documents, data and copies of documents on the proof of the client's identity, documents on the determination of the ownership of the means used by the client to conclude the insurance contract, the insurance contracts and documents related to the conclusions and administration of the insurance contracts during the insurance period and after the insurance termination until expiry of the lapse period for the exercise of rights resulting from the insurance contract, although for at least ten years after the termination of the contractual relation with the client; from damage, change, destruction, loss,*

theft, revealing, abuse and unauthorised access. The reinsurance company, branch of the reinsurance company from another member State and branch of a foreign reinsurance company shall be obliged to maintain and protect the reinsurance contracts including changes and related documents during the reinsurance period and after the reinsurance termination at least until expiry of the lapse period for the exercise of rights resulting from the reinsurance contract; from damage, change, destruction, loss, theft, revealing, abuse and unauthorised access".

425. Finally, the Act on Financial Intermediation and Financial Counselling and on amendments and supplements to certain laws (Article 31, paragraph 3 and 6) and Article 36) contain similar provisions.

426. Authorities indicated that, in practice, financial institutions keep all records regarding the transactions performed for at least 10 years on the basis of said sectoral laws and anything in the sectoral laws including record-keeping obligation is a sanctionable requirement. It must be noted that the Act on Banks, the Act on Securities, the Act on Insurance, the Act on Payment Services, the Act on Financial Intermediation and Financial Counselling and the Act on Collective Investment state that the NBS can dispose corrective measures and fines in its supervisory tasks when detecting the non compliance with the AML/CFT Act.

Record keeping of identification data, files and correspondence (c.10.2)

427. As required under essential criterion 10.2*, identification data, account files and business correspondence are within the scope of record-keeping obligation. Although the Slovak Authorities argue that the broad language of Section 19 of the AML/CFT Act involves such data (account files and business correspondence), evaluators consider there is no explicit and sufficient provision referring to these specific kind of documents, neither in the AML/CFT Act nor in the sectoral Acts that are referred to above. As noted in paragraph 462, financial institutions are required to keep identification data for at least five years after the business relationship with the customer is ended or longer if requested by a competent authority.

Availability of records to competent authorities in a timely manner (c.10.3)

428. According to Section 21 of the AML/CFT Act, obliged entities are requested to provide the FIU upon its written request with data on transactions, related documents, and information on persons, who participated in the transaction. In such cases, the FIU determines the time in which such a request must be submitted. Article 2, paragraph 7 of the Act on Supervision of the Financial Market refers to the availability of records to competent authorities, but does not contain a specific provision regarding the time in which this records should be available to the said authorities. Besides, Article 42, paragraph 2 of the Act on Banks states that "*Data and other information in returns, notifications and other reports must be comprehensible, easy to follow, supportable, and give a true and fair picture of reported facts, and must be presented in a time."* Article 75 (4) of the Securities Act, in conjunction with paragraph 6, requires that securities dealers and foreign securities dealers shall retain the records referred to in paragraphs (1) and (2) and any other documentation on its provision of investment or ancillary services in a medium that allows the storage of information in a way accessible for future reference by the National Bank of Slovakia, and in such a form and manner that the following conditions are met:

a) the National Bank of Slovakia must be able to access them readily and to reconstruct each key stage of the processing of each transaction;
b) it must be possible for any corrections or other amendments, and the contents of the records prior to such corrections or amendments, to be easily ascertained;
c) it must not be possible for the records otherwise to be manipulated or altered.

429. Finally, in the case of information or data requested in the course of criminal investigations, Section 3 of the CPC and Section 76 of the Act on Police Force state as "without delay" the deadline for the provision of the referred information.

430. The obligation for financial institutions to provide customer identification data (as well as transaction records) to the police is covered in paragraph 4 (g) of Section 91 the Act on Banks which states *"A report on matters concerning a client that are subject to bank secrecy shall be submitted by a bank or branch office of a foreign bank without the prior approval of the client concerned solely upon request made in writing by the criminal police and financial police services of the Police Corps for the purposes of detecting criminal acts, the detection of and search for their perpetrators and especially in the case of tax evasion, illegal financial operations, and money laundering."* Finally, on the basis of the paragraph 4 Section 29 (a) of the Police Act the police officer belonging to the Criminal or Financial Police is authorised to request from banks and foreign bank branches the reports on their customer identification data by detecting tax evasions or unlawful financial operations or legalisation of proceeds of criminal activity and thereto related criminal offences and their perpetrators.

431. Additional information to unusual transaction report shall be provided to the FIU by the obliged entity based on the written request under paragraph 5 of Section 17 of the AML/CFT Act.

432. Apart from these provisions, in the Slovak legislation, there is no clear requirement for financial institutions to ensure that all customer and transaction records and information are available on a timely basis to domestic competent authorities upon appropriate authority. The evaluation team was advised during the on-site visit by the private sectors' representatives that the time needed, in practice, to provide competent authorities with information requested depends on circumstances. Thus, the evaluators noted that some obliged entities may not have an efficient internal procedure to promptly satisfy information requests.

Effectiveness and efficiency

433. The requirements as stated in Section 19, paragraph 2 of the AML/CFT Act remain too general compared to essential criteria c.10.2* as understood by the FATF.

434. Effectiveness of the implementation of Recommendation 10 can be regarded as being sufficient. Controls performed at obliged entities between 2006 and 2010 by the Slovak FIU did not reveal any breach of AML-CFT Act regarding the obligation of transaction data recording

435. However, it must be noted that in practice, in the Slovak banking sector, documents are too often kept in paper form, which makes it difficult to retrieve information in a timely manner.

Special Recommendation VII (rated PC in the 3rd round MER)

Obtain Originator Information for Wire Transfers (c.VII.1)

436. Requirements under SR. VII have been implemented within the EU through Regulation (EC) No. 1781/2006, in force since 1 January 2007. This Regulation is directly applicable throughout the EU membership, including Slovakia.

437. According to Article 3 of the EU Regulation, it applies to transfers of funds, in any currency, which are sent or received by a payment service provider established in the EU. The Regulation does not apply to:

- transfers of funds carried out using a credit or debit card under specific conditions (Article 3, paragraph 2), electronic money up to a threshold of €1.000 (Article 3(3));

- transfers of funds carried out by means of a mobile phone or similar device (Article 3, paragraphs 4 and 5);
- cash withdrawals, transfers related to certain debit transfer authorisations, truncated cheques, transfers to public authorities for taxes, fines, or other levies within a member state;
- transfers, where both the payer and the payee are payment service providers acting on their own behalf (Article 3, paragraph 7).

438. According to Article 5 of the Regulation, providers shall ensure that transfers of funds are accompanied by complete information on the payer. This complete information on the payer includes the name, address and account number of the customer (Article 4).

439. The payment service provider of the payer shall, before transferring the funds, verify the complete information on the payer on the basis of documents, data or information obtained from a reliable and independent source (Article 5 (2)). In the case of transfers of funds not made from an account, the payment service provider of the payer shall verify the information on the payer only where the amount exceeds €1,000, unless the transaction is carried out in several operations that appear to be linked and together exceed €1,000 (Article 5 (4) of the Regulation). The general rules set out in the AML/CFT Act apply for this verification.

440. However, the EU Regulation also provides for some exemptions from the verification requirements if:

- a payer's identity has been verified in connection with the opening of the account and the information obtained by this verification has been stored in accordance with the obligations set out in the 3rd EU AML Directive; or
- the payer is an existing customer whose identity has to be verified at an appropriate time as described under Article 9(6) of the 3rd EU AML Directive.

Inclusion of Originator Information in Cross-Border Wire Transfers (c. VII.2); Inclusion of Originator Information in Domestic Wire Transfers (c. VII.3); Maintenance of Originator Information (c.VII.4)

441. According to the FATF Methodology, transfers between Slovakia other EU Member States are considered as domestic for the purposes of the assessment of SR. VII, wire transfers between Slovakia and non-EU Member States are considered as cross-border.

442. Therefore, according to Article 7 (1) of the Regulation, transfers where the payment service provider of the payee is situated outside the area of the EU shall be accompanied by complete information on the payer. In cases of batch transfers, it is not necessary to attach the complete information to each individual wire transfer provided that the batch file contains that information and that the individual transfers carry the account number of the payer or a unique identifier.

443. In cases where both the payment service provider of the payer and the payment service provider of the payee are situated in the Community, transfers of funds shall be required to be accompanied only by the account number of the payer or a unique identifier allowing the transaction to be traced back to the payer. If so requested by the payment service provider of the payee, the payment service provider of the payer shall make available to the payment service provider of the payee complete information on the payer, within three working days of receiving that request (Article 6 of the Regulation).

444. According to Article 14 of the Regulation, payment service providers shall respond fully and without delay to enquiries from the competent authorities concerning the information on the payer accompanying transfers of funds and corresponding records, in accordance with the procedural requirements established in the national law of the Member State in which they are situated. For the purpose of the EU Regulation, the competent authority in Slovakia is the FIU.

445. Article 12 of the Regulation stipulates that intermediary payment service providers shall ensure that all information received on the payer that accompanies a transfer of funds is kept with the transfer. In cases of technical limitations to a payment system, an intermediary payment service provider situated within the EU must keep records of all information received for five years (article 13 (5) of the Regulation).

Risk-based Procedures for Transfers Not Accompanied by Originator Information (c. VII.5)

446. As stipulated in Article 8 of the Regulation, the payment service provider of the payee shall detect whether, in the messaging or payment and settlement system used to affect a transfer of funds, the fields relating to the information on the payer have been completed. Providers shall have effective procedures in place in order to detect whether the following information on the payer is missing:

- for transfers of funds where the payment service provider of the payer is situated in the EU, the information required under Article 6;
- for transfers of funds where the payment service provider of the payer is situated outside the Community, complete information on the payer, or where applicable, the information required under Article 13; and
- for batch file transfers where the payment service provider of the payer is situated outside the Community, complete information on the payer in the batch file transfer only, but not in the individual transfers bundled therein.

447. If the payment service provider of the payee becomes aware, when receiving transfers of funds, that information on the payer required under this Regulation is missing or incomplete, it shall either reject the transfer or ask for complete information on the payer.

448. Where a payment service provider regularly fails to supply the required information on the payer, the payment service provider of the payee shall take steps, which may initially include the issuing of warnings and setting of deadlines, before either rejecting any future transfers of funds from that payment service provider or deciding whether or not to restrict or terminate its business relationship with that payment service provider. The payment service provider of the payee shall report that fact to the authorities responsible for combating money laundering or terrorist financing which is the FIU in Slovakia (Article 9 of the Regulation).

449. Pursuant to Article 10 of the Regulation, the payment service provider of the payee shall consider missing or incomplete information on the payer as a factor in assessing whether the transfer of funds, or any related transaction, is suspicious, and whether it must be reported, in accordance with the reporting obligations set out in the Third EU AML/CFT Directive, to the authorities responsible for combating money laundering or terrorist financing.

Monitoring of Implementation (c. VII.6) and Application of Sanctions (c. VII.7: applying c.17.1 – 17.4)

450. The competent authority in the Slovak Republic to effectively monitor, and take necessary measures with a view to ensuring compliance with the requirements of the EU Regulation is the NBS, according to the notification filed by the Slovak authorities to the EU Commission. This responsibility can also be derived from Section 50 of the Act on Banks.

451. The evaluation team was advised that the compliance with the Regulation is also verified by the NBS during on-site visits; however there has been only one case of verification in 2010. Rules on effective, proportionate and dissuasive penalties applicable to infringements of the provisions of the Regulation are set out in paragraphs 2 and 3 of Article 78 of the Act on Payment Services, and may be enforced by the NBS, as well as art. 50 of the Banking Act.

Additional elements – Elimination of thresholds (c. VII.8 and c. VII.9)

452. For transfers of funds where the payment service provider of the payer is situated outside the EU (incoming cross-border wire transfers), the payment service provider of the payee shall have effective procedures in place in order to detect whether the complete information on the payer as referred to in Article 4 (complete information on the payer) is missing (Article 8 (b) of the Regulation). If this is not the case, the payment service provider has to follow the procedures described above, regardless of any threshold (exemptions in context with batch file transfers are elaborated above).

453. For transfers of funds where the payment service provider of the payee is situated outside the area of the EU (outgoing cross-border wire transfers), the transfer shall always being accompanied by complete information on the payer, regardless of the threshold (Article 7 of the Regulation; exemptions in context with batch file transfers are elaborated above).

Effectiveness and efficiency

454. The requirements of SR. VII are clearly stated in the EU Regulation, respectively under the AML/CFT Act where necessary. It is also worth mentioning that the NBS published on its website the "Common Understanding Paper" both in English and Slovak (developed and published by the Anti-Money Laundering Task Force in October 2008 (established in 2006 by 3L3 Committees - CEBS, CEIOPS and CESR).

455. All representatives of providers of payment services met during the on-site visit appeared to be aware of their obligations when conducting transfers of funds. There were, however, no reports on regular failings of payment service providers filed with the FIU according to Article (2) of the Regulation.

456. It is a concern of the evaluation team that as at the time of the on-site visit, the NBS had just started to verify the compliance of financial institutions with the said Regulation during its on-site inspections (one case in 2010). There were no circumstances brought to the attention of the evaluation team that could by any way undermine the proper functioning of the supervision over the wire transfer system in Slovakia. Nevertheless, due to the above mentioned fact of a small number of NBS on-sites covering this issue, the effectiveness can not be assessed. The evaluation team is, however, satisfied that the financial institutions observe the obligations of the mentioned Regulation.

3.4.2 Recommendation and comments

Recommendation 10

457. Though different sectoral laws have provisions and authorities see no problem in practice, authorities should consider to establish a clear obligation upon financial institutions in the AML/CFT Act with a view to ensuring that transaction records to be kept are sufficient as required under essential criterion 10.1.1.

458. Section 19 of the AML/CFT Act should be amended to explicitly require the keeping of account files and business correspondence for at least five years following the termination of an account or business relationship.

Special Recommendation VII

459. This recommendation is fully observed.

3.4.3 Compliance with Recommendation 10 and Special Recommendation VII

	Rating	Summary of factors underlying rating
R.10	**LC**	• Record keeping obligation does not clearly require the maintenance of "account files and business correspondence".
SR.VII	**C**	

Unusual and Suspicious transactions

3.5 Monitoring of Transactions and Relationship Reporting (R. 11 and R. 21)

3.5.1 Description and analysis[10]

Recommendation 11 (rated NC in the 3rd round MER)

Special attention to complex, unusual large transactions (c. 11.1)

460. As indicated in the 3rd round MER, Slovakia has a reporting mechanism in effect for complex or unusual transactions. Section 14 of the new AML/CFT Act has broadly implemented the requirements of Recommendation 11. Requirements of paying special attention to all complex, unusual large transactions or unusual patterns of transactions, which have no apparent economic or visible place, and of examining the background and purpose of such transactions as well as setting forth their findings in writing have been provided for in this Section. Furthermore, Section 4 of the AML/CFT Act does provide detailed description of some typical unusual transactions.

Examination of complex and unusual transactions (c. 11.2)

461. The Slovak legal system now explicitly requires the obliged entities to examine the purpose of transactions to the most extent possible and to write up a written report on such transactions (paragraph 3 of Section 14 of the AML/CFT Act)

Record-keeping of finding of examination (c. 11.3)

462. While the said section obliges financial institutions to make their written findings available when a control is being conducted under Section 29 of the AML/CFT Act, the Act does not include an explicit obligation for them to keep those reports for at least five years. Such an obligation may be drawn neither from the Section 29 nor Section 14 of the AML/CFT Act. This deficiency has not been rectified since the 3rd round evaluation. The FIU has, however, issued guideline soon after the AML/CFT Act came into force in 2008 (Guidelines for obliged entities related to observance of obligations stipulated in Section 14 of AML/CFT Law in connection with detection of unusual transaction) that requires the institutions to keep the findings of examination of transactions for the period of five years. However, this guideline is not an other enforceable means.

463. The evaluation team is satisfied that financial institutions know their obligation arising from Section 14 of the AML/CFT Act, and that the screening of transactions is done with proper diligence. Nevertheless, the awareness raising activities by the NBS and the FIU should continue in this matter, though the methodological guidance provided by the NBS is quite comprehensive.

[10] The description of the system for reporting suspicious transactions in s.3.7 is integrally linked with the description of the FIU in s.2.5, and the two texts need to be complementary and not duplicative.

Recommendation 21 (rated NC in the 3rd round MER)

Special attention to countries not sufficiently applying FATF Recommendations (c. 21.1 & 21.1.1), Examination of transactions with no apparent economic or visible lawful purpose from countries not sufficiently applying FAT Recommendations (c 21.2)

464. One of the deficiencies identified in the 3rd round MER was the absence of any broad requirement for financial institutions to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations. This appears not to have been remedied yet.

465. The Slovak authorities indicated that the risk-based approach is embedded in paragraph 4 of Section 10 and paragraph 2 of Section 14 of the AML/CFT Act. However, in the absence of an explicit requirement, it is not clear that those provisions require obliged entities to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations. The authorities report that in practice, public statements of the FATF and MONEYVAL are published on the FIU's web-site and they are considered by the financial institutions. However, this should be explicitly set out in law, regulation or other enforceable means.

466. The only guidance provided to financial institutions by a competent authority (Slovak FIU website) is the "Guidelines for obliged entities in connection with FATF Statements and MONEYVAL", which instruct obliged entities to follow the procedure under Section 12 (1) or (2) (b) and (c) of AML/CFT Act (EDD) and to apply not only CDD but also other measures to eliminate the risks identified. The evaluation team considers that there are not sufficient measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries. Besides, there is no specific obligation for financial institutions to examine the background and purpose of transactions that have no apparent economic or visible lawful purpose and to make available the written findings to assist competent authorities. (c. 21.2).

Ability to apply counter measures with regard to countries not sufficiently applying FATF Recommendations (c 21.3)

467. The current legal framework of the Slovak Republic does not give power to any national authority to apply any countermeasures whatsoever, within the scope of Recommendation 21.

Effectiveness and efficiency

468. In the Slovak Law, there is not a general provision concerning the obligation of financial institutions to pay special attention to any country that fails or insufficiently applies FATF Recommendations. Slovak authorities are not currently in a position to apply countermeasures.

469. Obliged entities should be aware by their own sources of weaknesses in the AML/CFT systems of other countries. Thus, effective compliance with Recommendation 21 is difficult to be asserted.

3.5.2 Recommendations and comments

Recommendation 11

470. A term for keeping written findings should be determined by law, regulation or other enforceable means with a view to ensure that financial institutions keep available such findings for at least five years.

Recommendation 21

471. There should be effective measures in place to ensure that financial institutions are advised of concerns about weakness in the AML/CFT systems of other countries.

472. The Slovak legal framework should include a general provision concerning the obligation of financial institutions to pay special attention to business relationships and transactions with persons from or in countries that fail or insufficiently apply FATF Recommendations.

473. In particular, the Slovak AML/CFT legal framework should include a provision concerning the obligation for entities to examine as far as possible those transactions that have no apparent economic or visible lawful purpose and to make written findings available to assist competent authorities (e.g. supervisors, law enforcement agencies and the FIU) and auditors.

474. The Slovak authorities should be legally empowered to apply counter-measures within the meaning of Recommendation 21.

3.5.3 Compliance with Recommendation 11 and Special Recommendation 21

	Rating	Summary of factors underlying rating
R.11	**LC**	• No enforceable keeping term for written findings on unusual transactions exists.
R.21	**NC**	• No enforceable requirement for financial institutions to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations. • No effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries. • No mechanisms in place that would enable the authorities to apply counter-measures to countries that do not apply or insufficiently apply FATF recommendations. • No requirement to examine, as far as possible, the background and purpose when transactions have no apparent economic or visible lawful purpose, and to make available written findings to assist competent authorities and auditors.

3.6 Suspicious Transaction Reports and Other Reporting (R. 13, 19, 25 and SR.IV)

3.6.1 Description and analysis

Recommendation 13 (rated PC in the 3rd round MER) & Special Recommendation IV (rated NC in the 3rd round MER)

Requirement to Make STRs on ML/FT to FIU (c. 13.1, c.13.2 & IV.1)

475. Slovakia was rated *"Partially Compliant"* in the 3rd round MER stating that even though there was a direct mandatory reporting requirement in the AML/CFT Act, the reporting system was not clear, attempted transactions were not covered and no guidance for reporting entities were issued. Though significant improvements in reporting system are evident since the 3rd round evaluation, some deficiencies spotted at that time remain.

476. Reporting entities are obliged to report unusual transactions according to Section 17 of the AML/CFT Act. Paragraph 1 of the stated article reads as follows: "Obliged entity shall report to the Financial Intelligence Unit an unusual transaction or attempt to make such a transaction without undue delay. Obliged entity shall report to the Financial Intelligence Unit without undue delay also refusal to carry out the required unusual transaction under Section 15." Section 15 of the AML/CFT Act deals with the refusal of or termination of a business relationship or refusal to execute a transaction when CDD measures cannot be implemented.

477. The AML/CFT Act defines an unusual transaction as a "legal act or other act which indicates that its execution may enable legalisation or terrorist financing." (Section 4)

478. When it comes to definitions of money laundering (the term used in the AML/CFT Act is "legalisation"), it is stated under Section 2 of the AML/CFT Act that for the purpose of this Act ML shall be understood "*intentional conduct consisting in*

a) conversion of nature of property or transfer of property, knowing that the property originates from criminal activity or involvement in criminal activity, with the aim of concealing or disguising the illicit origin of the property or with the aim of assisting a person involved in the commission of such criminal activity to avoid the legal consequences of his conduct,

b) concealment or disguising of the origin or nature of property, the location or movement of property, the ownership or other title to property, knowing that the property originates from criminal activity or involvement in criminal activity,

c) acquisition, possession, use and handling of property, knowing that the property originates from criminal activity or involvement in criminal activity,

d) involvement in action under letters a) to c), even in the form of association, assistance, instigation and incitement, as well as in attempting such action."

479. The evaluators conclude from the previous articles that reporting entities in Slovakia are obliged to report any kind of acts when they suspects that its execution may enable ML or TF. Bearing in mind that the all-crime-approach is used in the ML definition, it can be concluded that obliged entities are required to report any activity which raises suspicion that proceeds from any crime are involved in its execution.

480. The AML/CFT Act goes further in defining unusual transaction, implicitly providing reporting entities with some guidance or indicators for recognising suspicion. Paragraph 2 of Section 4 of the AML/CFT Act further states that: "*unusual transaction shall mean especially a transaction*

a) which with regard to its complexity, unusually high amount of funds or its other nature, goes apparently beyond the common framework or nature of a certain type of transaction or a transaction of a certain customer,
b) which with regard to its complexity, unusually high amount of funds or its other nature, has no apparent economic purpose or visible lawful purpose,
c) where the customer refuses to identify himself or to provide the information necessary for the obliged entity to perform customer due diligence under Sections 10 to 12,
d) where the customer refuses to provide information of the upcoming transaction or tries to provide as little information as possible or shall provide such information that obliged entity can verify with great difficulty or only with vast expenses,
e) where the customer demands its execution based on a project which raises doubts,
f) where money of low nominal value in a considerably high amount are used,
g) with a customer in whose case it can be presumed that with regard to his occupation, position or other characteristics, he is not or cannot be the owner of the required funds,
h) where the amount of funds that the customer disposes of is in apparent disproportion to the nature or scope of his business activity or financial status declared by him,
i) where there is a reasonable assumption that the customer or beneficial owner is a person on whom international sanctions are imposed under a special regulation11 or a person who might be related to a person on whom international sanctions are imposed under a special regulation; or
j) where there is a reasonable assumption that its subject is or is to be an object or a service that may relate to an object or a service on which international sanctions are imposed under a special regulation[12].”

481. Apart from these indicators or examples of unusual transactions, which are instructive but rather general, the banking sector has received further guidance regarding possible forms of unusual transactions. These indicators are given in the Annex to the Methodological Guideline of 17 December 2009 No 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing. However, no other reporting entities are provided with this kind of guidance.

482. The obligation to report unusual transaction has to be fulfilled “without undue delay”. This provision is enforced in practice since reports are received in due time, usually on the same day. One reporting entity advised the evaluators that the FIU has imposed a penalty for non-compliance with this provision of the AML/CFT Act. Furthermore, obliged entities are required to postpone an unusual transaction if there is a danger that its execution may hamper or substantially impede seizure of proceeds of criminal activity or funds intended to finance terrorism. Authorities advised the evaluators that transactions are postponed by reporting entities till the report is made.

483. The AML/CFT Act provides also for the manner of reporting stating that: “*Reporting duty shall be fulfilled:*
a) in person,
b) in writing,
c) electronically or
d) by phone if the matter brooks no delay; such a report is necessary to file also in person, in writing or electronically within three days from receipt of the phone call by the Financial Intelligence Unit.”

[11] Act No. 460/2002 Coll. on the Application of International Sanctions Assuring International Peace Settlement and Security as amended by Act No. 127/2005 Coll.
[12] Act No. 460/2002 Coll. on the Application of International Sanctions Assuring International Peace Settlement and Security as amended by Act No. 127/2005 Coll.

484. The Act requires that an unusual transaction report shall include:

a) obliged entity's business name, registered office or place of business and identification number,
b) data obtained by the identification of persons to whom the unusual transaction concerns,
c) data about the unusual transaction, especially the reason of its unusualness, the time sequence of events, account numbers, information when the accounts were opened, who their owner is and who has the right of disposal to them, photocopies of documents on the basis of which the accounts were opened, identification data of persons authorised to dispose of the accounts, photocopies of the concluded contracts and other related documents and information, as well as other information that may be related to the unusual transaction and are essential for its further examination,
d) data on third persons possessing information on the unusual transaction,
e) name and surname of the compliance officer and phone contact of this person

485. It is stated also that the reporting obligation shall not be restricted by the obligation of keeping secrecy specified by the law under special regulations.

486. The obligation to report unusual transaction extends to transactions that are linked to terrorism financing since the definition of UTR in Article 4 of the AML/CFT Act covers also the acts the execution of which may result in terrorist financing. By the adoption of the new AML/CFT Act terrorist financing is now covered in suspicious transaction reporting. For the purposes of the AML/CFT Act, terrorist financing is defined as "*provision or collection of funds with the intention of using them or knowing that they are to be used, in whole or in part, to commit:*

a) the criminal offence of establishing, contriving and supporting a terrorist group or the criminal offence of terrorism or
b) the criminal offence of theft, the criminal offence of extortion or the criminal offence of counterfeiting and altering a public document, official stamp, official seal, official die, official sign and official mark or of instigating, aiding or inciting a person to commit such a criminal offence or his attempt aimed to commit a criminal offence of establishing, contriving and supporting a terrorist group or the criminal offence of terrorism."

487. The definition of TF does not contain financing of an individual terrorist. The definition also does not cover the financing of the acts defined in the treaties annexed to the TF Convention. These shortcomings are considered to be a limitation to the reporting regime as well. Reporting entities are lacking legal basis to report unusual transaction which is connected with an individual terrorist. Furthermore, the AML/CFT Act does not specifically require reporting funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism, as required under criterion 13.2.

No Reporting Threshold for STRs (c. 13.3 & c. SR.IV.2)

488. The AML/CFT Act explicitly requires obliged entities to report all unusual transactions including attempted transactions. Since the AML/CFT Act does not determine any threshold for unusual transactions, the reporting obligation applies irrespective of any threshold.

Making of ML/FT STRs regardless of Possible Involvement of Tax Matters (c. 13.4, c. IV.2)

489. Obliged entities are required to report any acts which indicate that its execution may enable legalisation of proceeds from any criminal offence. Tax fraud is regarded as criminal activity that is punishable in the Slovak Criminal Code. Therefore, it is a predicate offence for ML as well. Slovak legislation does not provide for any exception for unusual transaction reporting requirement by reason of tax related matters. Hence, the reporting obligation applies regardless of whether the transaction, among other things, involves tax matters.

Additional Elements – Reporting of All Criminal Acts (c. 13.5)

490. Slovakia introduced an all crime approach, thus all obliged entities are required to report when they suspect or have reasonable grounds to suspect that fund are proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically.

Special Recommendation IV

491. Reporting entities are obliged to report unusual transactions on TF according to Section 17 of the AML/CFT Act. Paragraph 1 of the stated article reads as follows: "*Obliged entity shall report to the Financial Intelligence Unit an unusual transaction or attempt to make such a transaction without undue delay. Obliged entity shall report to the Financial Intelligence Unit without undue delay also refusal to carry out the required unusual transaction under Section 15."* Section 15 of the AML/CFT Act deals with the refusal of or termination of business relationship or refusal to execute transaction when CDD measures cannot be implemented.

492. The AML/CFT Act defines unusual transaction as a *"legal act or other act which indicates that its execution may enable legalisation or terrorist financing."* (Section 4)

493. The obligation to report unusual transaction extends to transactions that are linked to terrorism financing since the definition of UTR in Article 4 of the AML/CFT Act covers also the acts the execution of which may result in terrorist financing. By the adoption of the new AML/CFT Act terrorist financing is now covered in suspicious transaction reporting. For the purposes of the AML/CFT Act, terrorist financing is defined as *"provision or collection of funds with the intention of using them or knowing that they are to be used, in whole or in part, to commit:*

a) the criminal offence of establishing, contriving and supporting a terrorist group or the criminal offence of terrorism or
b) the criminal offence of theft, the criminal offence of extortion or the criminal offence of counterfeiting and altering a public document, official stamp, official seal, official die, official sign and official mark or of instigating, aiding or inciting a person to commit such a criminal offence or his attempt aimed to commit a criminal offence of establishing, contriving and supporting a terrorist group or the criminal offence of terrorism."

494. As noted above, the definition of TF in the AML/CFT Act does not contain financing of an individual terrorist. This shortcoming is considered to be a limitation to the reporting regime as well. Reporting entities are lacking legal basis to report unusual transaction which is connected with an individual terrorist. Furthermore, the AML/CFT Act does not specifically require the reporting of funds where there are reasonable grounds to suspect or they are suspected to be linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

495. The AML/CFT Act provides some examples on what specifically should be considered as an unusual transaction with regard to terrorist financing. These situations are:

"i) where there is a reasonable assumption that the customer or beneficial owner is a person on whom international sanctions are imposed under a special regulation[13] or a person who

[13] Act No. 460/2002 Coll. on the Application of International Sanctions Assuring International Peace Settlement and Security as amended by Act No. 127/2005 Coll.

might be related to a person on whom international sanctions are imposed under a special regulation[14] or

j) where there is a reasonable assumption that its subject is or is to be an object or a service that may relate to an object or a service on which international sanctions are imposed under a special regulation[15].

496. As no other indicators for recognising unusual transactions related to TF have been issued, reporting entities could only rely on these two provided in the Act. The evaluators also got the impression that obliged entities reported unusual transactions that are only linked to persons or geographical areas which were related to international sanctions. Law enforcement bodies met on-site which receive these reports from the FIU confirmed this impression.

497. As elaborated above under R.13, the reporting obligation is applicable for attempted transactions that are suspected to be linked to TF, and no exception is provided to the unusual transaction reporting requirement by reason of tax related matters.

Effectiveness and efficiency (R.13-SRIV)

498. The reporting level from banking and to some extent the insurance sector appears to be satisfactory. However, other financial institutions show a significantly lower level of reporting.

499. It has already been mentioned that some guidance in that regard is presented in the AML/CFT Act itself. Apart from guidance or indicators given in this Act the Slovak authorities have provided the evaluators with the guidance in a form of indicators for recognising UTRs that are published by the FIU on its web site. These indicators are consisted of 10 "General ways of recognising UT", 23 "specific ways" in bank activities, 16 for insurance companies, 15 for leasing activities, 13 for auditing and accounting activities, 9 for executor's activities, 3 for public carriers and forwarding activities and 5 for real estate activities. Indicators for the banking sector are also presented in the Methodological guidance. However, no other sectors have been provided with this kind of guidance.

500. Only banks have submitted reports on TF. Furthermore, there are no specific guidance and indicators in place for obliged entities on reporting TF.

Table 13: Breakdown of UTRs received by the FIU

Monitoring entities, e.g.	reports about unusual transactions		reports about unusual transactions		reports about unusual transactions		reports about unusual transactions		reports about unusual transactions	
	ML	FT	ML	FT	ML	FT	ML	FT	ML	FT
	2006		2007		2008		2009		2010	
Commercial banks	1,313	14	1,757	9	1,926	16	2,321	56	1976	55
Insurance companies	151	0	147	0	261	0	115	0	85	0
Notaries	0	0	0	0	5	0	2	0	1	0
Currency exchange	1	0	0	0	0	0	0	0	0	0
Broker companies	30	0	0	0	0	0	27	0	13	0

[14] Act No. 460/2002 Coll. on the Application of International Sanctions Assuring International Peace Settlement and Security as amended by Act No. 127/2005 Coll.

[15] Act No. 460/2002 Coll. on the Application of International Sanctions Assuring International Peace Settlement and Security as amended by Act No. 127/2005 Coll.

Securities' registrars	4	0	0	0	7	0	4	0	1	0
Lawyers	1	0	0	0	0	0	0	0	1	0
Accountants	0	0	0	0	1	0	1	0	2	0
Auditors	0	0	0	0	1	0	3	0	1	0
Tax advisors	0	0	0	0	0	0	1	0	2	0
Company service providers	0	0	0	0	0	0	2	0	5	0
Post office	2	0	1	0	4	0	11	0	102	0
Financial regulators	0	0	0	1	0	0	49	0	46	0
Car dealers	53	0	29	0	49	0	1	0	43	0
Bookmakers	1	0	0	0	0	0	5	0	26	0
Executor	1	0	0	0	2	0	1	0	1	0
Casinos/Gambling game operator	0	0	0	0	0	0	2	0	7	0
Natural or legal persons authorised to trade in receivables	0	0	0	0	0	0	12	0	10	0
Natural or legal persons authorised to provide forwarding services	0	0	0	0	2	0	0	0	1	0
Money transmitter (Western Union)	0	0	0	0	0	0	1	0	27	0
Leasing companies	0	0	0	0	0	0	68	0	47	0
Real estate agencies	0	0	0	0	0	0	2	0	2	0
Auctions out of distrainments	0	0	0	0	0	0	0	0	0	0
Asset management companies	0	0	0	0	0	0	2	-	16	0
Others	0	0	0	0	0	0	0	0	0	0
Total	*1,557*	*14*	*1,934*	*10*	*2,257*	*16*	*2,683*	*56*	*2415*	*55*

Recommendation 25(c. 25.2 – feedback to financial institutions on STRs rated NC in the 3rd round MER)

501. With regard to feedback to reporting entities, Slovak authorities reported in the MEQ that feedback is provided for as follows:

- general feedback – annual report as well as feedback to each credit institution quarterly and
- specific (case-by-case) feedback on a request of a reporting entity or based on an initiative of the FIU respectively.

502. It should be noted that Section 26/2(i) requires the FIU to provide obliged entities with case-by-case feedback.

503. The financial institutions met on-site confirmed that they receive tables with information related to the UTRs submitted by them, quarterly. The same information is provided to DNFBPs twice a year. The evaluators have been provided with two examples of the mentioned tables. The first one was provided by a reporting entity interviewed on-site which contains data provided to that reporting entity from the FIU in 2009. The feedback that is provided in this table contains general information on UTRs submitted (number of UTRs, date of submitting etc.), transaction amounts and the results of the analysis. Regarding results, reporting entities received information on the date of finishing the analysis and information whether the report is sent to law enforcement authorities for further investigation. There was no information on whether the law enforcement body has continued the investigation and no any other substantive information on the case which could help the reporting entity in its further work. Some conclusions on the quality of reports could be drawn from the information given by the FIU, but that cannot be considered as the information that is

useful for enabling reporting entities to advance their systems, since no information on typologies or sanitised examples of actual cases are provided. Nevertheless, the FIU has provided the evaluators with another example of the table with feedback which is sent to a reporting entity in 2010. This table contains all the data described above, but in addition, it contains also information on results that are accomplished by law enforcement authorities according to each unusual transaction reported. As explained by authorities, this is new and developed practice that is in force at the moment. Evaluators welcome these improvements and encourage the FIU to continue with this work. Some feedback is also provided in a form of general feedback, by guidelines published on the FIU web site. These documents are already mentioned above. Although very brief, all of them contain valuable information for recognising unusual transactions in specified fields and valuable feedback because the cases described in them stem from the current FIU practice

504. Since the adoption of the 3rd round MER, the FIU has started to provide feedback to financial institutions on the STRs filed by them. Thus, feedback to reporting entities shows progress, particularly as financial institutions and DNFBPs receive tables on every UTR quarterly. Nonetheless, more substantial and descriptive information in respect of quality of the reporting would assist by way of additional feedback. Generally the content and promptness of the feedback is not fully satisfactory to the recipients. It was also clearly indicated that the financial institutions would appreciate more detailed feedback if permissible by law or other regulation.

Recommendation 19 (rated NC in the 3rd round MER)

Consideration of reporting of Currency transactions above a Threshold (c. 19.1)

505. Slovakia was rated "*Non-Compliant"* in the 3rd round MER in respect of R. 19 on the grounds that no consideration had been given to introducing a cash reporting system.

506. The Slovak system still does not require financial institutions to report all transactions in currency above a fixed threshold.

507. Recommendation 19 obliges countries to consider the feasibility and utility of implementing a system where financial institutions report all transactions in currency above a fixed threshold to a national central agency with a computerised database. It is the understanding of the evaluators that such consideration should be performed together by all relevant competent authorities in a country, preferably in a form of detailed risk analysis. It would be advisable to procure a document stating basic arguments in favour or against the fixed threshold reporting.

508. The Slovak authorities report that the issue was considered, but it was concluded that introduction of such a system was not a priority. The Slovak authorities have provided a written assessment of the feasibility and utility of implementing a system referred to in R.19. This issue was discussed in more detail at the IIGE´s meetings in 2008, and also on 18 February 2010. During these meetings consideration was given on the introduction of a cash reporting system by all relevant authorities in Slovakia (the FIU, the Ministry of Justice, the Ministry of Finance, the NBS, the General Prosecutor's Office, the State Secret Service, the Anti-Terrorist Unit, the Anti-Drug Unit, and the Tax Directorate of the Slovak Republic).

509. Some Slovak authorities met on-site advised the evaluators that cash economy in the country was on decrease since the introduction of the Euro as the currency of Slovakia.

Additional elements – Computerised database for currency transactions above threshold and access by competent authorities (c. 19.2)

510. N/A.

Additional Element – Proper use of Reports of Currency Transactions above Thresholds (c. 19.3)

511. N/A.

3.6.2 Recommendations and comments

Recommendation 13 and Special Recommendation IV

512. Guidelines for effective implementation of the reporting obligation are provided in the form of specific indicators for recognising unusual activities to banking, insurance and leasing sectors. They are listed in the annex to the Methodological Guideline of 17 December 2009 No 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing and in another document issued by the FIU and published on its website. Indicators given in the AML/CFT Act are rather general. Indicators for recognising suspicious transactions as guidelines for other financial sectors (securities market, currency exchange etc) are still needed and should be issued by the FIU and other competent bodies.

513. Not all designated categories of offences are fully covered as predicates, as incrimination of the financing of an individual terrorist is not covered. The Slovak authorities should take legislative measures in order to ensure that there is a clear obligation to report to the FIU when an obliged entity suspects or has reasonable grounds to suspect that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism.

514. Indicators for recognising unusual transactions regarding terrorist financing in the AML/CFT Act are limited to those in relation with international sanctions. Apart from these indicators presented in the Act and one another document issued by the FIU – "Guidelines for credit institutions related to potential way of terrorist financing", no other indicators for terrorist financing have been published. Authorities should take measures to provide the financial sector with a comprehensive set of guidelines for recognising suspicious transactions that are related to TF.

515. More guidelines to financial sector should be provided to the financial sector in order to improve the reporting regime.

Recommendation 25/c. 25.2 [Financial institutions and DNFBPs]

516. Progress has been achieved in relation to case-by-case feedback, particularly as financial institutions receive tables on every UTR quarterly. Together with the work of the FIU in providing general feedback in the form of guidelines containing trends and typologies, the picture in the area of feedback is improving constantly. Nonetheless, the Slovak authorities are encouraged to continue with their efforts in this field and to include more substantial and descriptive information in the tables that are already disseminated to reporting entities.

517. More focus should be placed on improving the co-operation with the DNFBP sector in the respect of feedback on STRs. The financial institutions are generally satisfied with the feedback they receive, but it is worth analysing whether the feedback should be more detailed and prompt, as it was one of the major concerns of the financial sector. The evaluators also strongly believe that prompt and detailed feedback can largely improve the effectiveness of implementing Recommendation 25.

Recommendation 19

518. This Recommendation is fully observed.

3.6.3 Compliance with Recommendations 13, 14, 19 25 and Special Recommendation SR.IV

	Rating	Summary of factors underlying rating
R.13	**PC**	• No clear reporting obligation 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 have an impact on the reporting of suspicious transactions. • Specific guidance or indicators for recognising suspicious transactions needed for all reporting institutions. • Effectiveness issues due to the fact that only banking and in some extent insurance sectors are reporting satisfactorily.
R.19	**C**	
R.25	**LC**	• The co-operation with the DNFBP is unsatisfactory. (25.2) • Feedback provided to reporting entities not always substantive and descriptive enough. (25.2)
SR.IV	**PC**	• No clear reporting obligation 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 limit the reporting obligation. • Indicators or guidelines to reporting entities limited to cases related to international sanctions. No specific indicators provided except two, presented in the AML/CFT Act and one another published on the FIU website. • Only banks reported UTRs regarding TF (effectiveness issues).

Internal controls and other measures

3.7 Internal Controls, Compliance, Audit and Foreign Branches (R.15 and 22)

3.7.1 Description and analysis

Recommendation 15 (rated PC in the 3rd round MER)

519. Section 20 of the new AML/CFT Act appears to broadly correspond with the requirements of Recommendation 15 in that there are obligations to create an internal control system, internal procedures, policies to prevent ML and TF, and to designate compliance officers (but not at management level).

Internal AML/CFT procedures, policies and controls (c. 15.1)

520. On the basis of Section 20 of AML/CFT Act the obliged entities must prepare in writing and update their own activity programmes aimed at the prevention of legalisation and terrorist financing. Beyond other issues, it must contain:

- way of performing customer due diligence,
- a procedure applied while evaluating whether the transaction being prepared or carried out is unusual,
- a procedure applied from the moment of detecting an unusual transaction to its immediate reporting to the FIU including procedure and responsibility of employees evaluating the unusual transaction,
- a procedure applied while postponing an unusual transaction,
- a procedure applied for the keeping of data.

521. Paragraph 3 of the same section requires financial institutions to ensure that the activity programme is permanently available to each employee performing the tasks under the AML/CFT Act.

522. Therefore, it can be concluded that the activity programmes of financial institutions include internal procedures, policies and controls to prevent ML and TF as required under c.15.1, and they communicate these to their employees. These have also been confirmed by the sectors' representatives interviewed during the on-site visit.

Compliance Management Arrangements (c. 15.1.1, 15.1.2)

523. On the basis of the AML/CFT Act the obliged entities are required to establish a "compliance officer" responsible for protection against money laundering and financing of terrorism (paragraph 2 (h) of Section 20). Compliance officers report unusual transactions to and keep contact with the FIU. On the basis of internal regulations, the obliged entities shall define the position of compliance officers and shall guarantee all their competences and powers to perform the duties specified by the Act. It is not clearly stated in the legislation that the compliance officer must be placed on a managerial level.

524. In part B of the Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing, there are more detailed supervisory expectations towards the position of a compliance officer, the range of his duty, his reporting lines, etc. This document states clearly that the compliance officer is the person who is responsible for the proper protection of the bank against money laundering and terrorist financing. As it is not set in a legally binding Act this cannot be properly enforced.

525. Furthermore, the AML/CFT Act does not provide for an explicit legal obligation requiring institutions to ensure that the compliance officer has timely access to CDD information, transaction records, and other relevant information. During the interviews with financial institutions' representatives the evaluation team was assured that even though such legal obligation does not exist, the compliance officers de facto have full timely access to CDD information, transaction records, and other information, which they may deem relevant.

Independent Audit Function (c. 15.2)

526. Financial institutions are obliged to control compliance with their own activity programmes aimed at the prevention of legalisation and terrorist financing and obligations stipulated in paragraph 2 (k) of Section 20 of the AML/CFT Act. The manner of performing control is stated in their own programmes.

527. Due to the application of the EU legislation in the field of financial institutions, all of the financial institutions are obliged by law to have an independent audit unit, or function for that matter (which is stated explicitly in respective special laws governing branches of the financial

market). All of the financial institutions are also required to have adequate resources to undertake their activities, which can be interpreted as an obligation to provide the resources needed, also to the audit function, as it is an essential part of any financial institutions' activities.

528. It should be mentioned, that considering payment service providers the provisions of law differ slightly, as to the name of the audit function. In Article 70 of the Act on Payment Services it is stated that the payment service providers should have an internal control. Article 70 defines internal control as the *"…control over compliance with laws and other generally binding legal provisions, the payment institution's articles of association, prudential rules and rules for protection against the laundering of proceeds from criminal activity and the financing of terrorism."*

529. Internal audit to test the AML/CFT measures' compliance is a part of general internal audit in the case of large financial institutions. For smaller ones, this obligation is rarely observed, with the exception of banks which have this obligation clearly stated in the Act on Banks.

Employee Training (c. 15.3)

530. Paragraph 3 of Section 20 of the AML/CFT Act requires financial institutions to provide for special training of employees aimed at making them aware of the programme, at least once a calendar year and always before the assignment of an employee to a job position requiring the fulfilment of tasks under the AML/CFT Act. The financial institutions are also obliged to ensure that the programme is permanently available to each employee performing the tasks under the AML/CFT Act.

531. During the on-site visit, the sectors' representatives interviewed declared that they provide their employees with special training, sometimes in co-operation with the Slovak authorities.

Employee Screening (c. 15.4)

532. In practice, before a new employee is hired, financial institutions generally require them to submit a clear criminal record. However, there has not yet been a legal obligation introduced, in law, regulation or other enforceable means, for financial institutions to put in place comprehensive screening procedures to ensure high standards when hiring employees.

533. The Slovak authorities stated that this policy is commonly determined by obliged entities' internal screening procedures.

Additional elements (c. 15.5)

534. Criterion 15.5 states whether the AML/CFT compliance officer is able to act independently and to report to senior management above the compliance officer's next reporting level or the board of directors.

535. This issue is not legally determined in Slovakia. The Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing (part B) formulates some recommendations on this topic.

536. In practice, banks' compliance officers are at a manager level as they report directly to the Board.

Effectiveness and efficiency

537. The AML/CFT Act appears now to correspond with the requirements of FATF Recommendation 15 in that there are obligations to create an internal control system, internal procedures, policies to prevent ML and TF, to designate compliance officers etc. (There are some uncertainties in the legislation while there are some improvements.)

538. The effectiveness of Recommendation 15 in the view of obligations arising from the Slovak legislation appears to be sufficient. The compliance function is set up properly, independently and correctly resourced, as the evaluation team was advised by the market participants. There is no problem with the compliance officers' access to information and documents which he may be in need of.

Recommendation 22 (rated PC in the 3rd round MER)

539. Recommendation 22 was rated *"Partially Compliant"* in the 3rd round MER due to the absence of a general obligation for financial institutions which ensures their branches and subsidiaries observe AML/CFT measures consistent with Slovak requirements and the FATF Recommendations to the extent that host country laws and regulations permit, and lack of any requirement to pay particular attention to situations where branches and subsidiaries are based in countries that do not or insufficiently apply FATF Recommendations. Absence of any provision that required branches and subsidiaries, where minimum AML/CFT requirements of the home and host countries differ, to apply the higher standard to the extent that local laws and regulations permit was another deficiency identified in the 3rd round MER.

540. Though in comparison with the situation at the time of the 3rd round evaluation some progress has been made concerning foreign branches and subsidiaries of financial institutions there are still deficiencies in place that have not been addressed.

541. Financial institutions in Slovakia are required to ensure that their foreign branches and subsidiaries located outside the territory of an EU Member State apply the measures equivalent to performing CDD under Section 10 to 12 of the AML/CFT Act and record-keeping under Section 19. However, this requirement applies to part of the FATF Recommendations (5 and 10) and does not extend the requirement to all of the FATF Recommendations.

542. There is no such requirement in respect of branches and subsidiaries of the institutions located in EU Member States. The Slovak authorities explained that it is presumed that AML/CFT obligations in EU Member States are equivalent to those existing in Slovakia due to the fact that all EU Member States are obliged to implement the 3rd EU AML/CFT Directive, hence branches and subsidiaries of Slovakia are considered to be also obliged entities under the relevant AML/CFT legislation of other EU Member States. Nevertheless, such obligation should be applied also to branches and subsidiaries in other EU Member States.

543. Financial institutions in Slovakia are required to inform the FIU when a foreign branch or subsidiary in countries that are not members of EU or the European Economic Area is unable to appropriately observe the practice of customer due diligence and record-keeping because this is prohibited by local (i.e. host country) laws, (Section 24 paragraph 3).

544. In cases of a discrepancy between Slovak and host country regulations, the obliged entity shall adopt appropriate supplementary measures to effectively mitigate the risk of exploitation for the ML and TF. There is, however, no requirement to apply the "higher standard", as required in essential criteria 22.1.2. Once again this requirement is limited to "third countries".

Additional elements (c. 22.3)

545. The provisions of Slovak Law do not clearly require financial institutions to apply consistent CDD measures at the group level, taking into account the activity of the customer with the various branches and majority owned subsidiaries worldwide. There were however no legal impediments to accepting this strategy.

Effectiveness and efficiency

546. At the time of the on-site visit only four Slovak financial institutions had branches or subsidiaries abroad, and all of them were located in EU Member States, which apply the same standards by the virtue of implementing the 3rd EU AML/CFT Directive. However, the limitation of this requirement to subsidiaries and branches in third countries (e.g. non-EU) significantly limits its scope. Overall, this has a material impact on the effectiveness of Recommendation 22 on branches and subsidiaries operating outside of Slovakia.

3.7.2 Recommendation and comments

Recommendation 15

547. The Slovak legal framework does not contain a provision concerning timely access of the compliance officer to customer identification data and other CDD information, transaction records and other relevant information, though this deficiency is partly addressed by the NBS Methodological guidance and the overall approach of the financial institutions. It is, however, advisable to clearly state such provision in the law, to ensure full compliance with R.15.

548. The Slovak authorities should also clearly state in law, regulation or other enforceable means that the compliance officer should be appointed at a managerial level.

549. The Slovak authorities should introduce a legal obligation in law, regulation or other enforceable means for financial institutions to put in place comprehensive screening procedures to ensure high standards when hiring employees.

Recommendation 22

550. It is recommended that Slovakia extend the requirements in Section 24 to the FATF Recommendations in general, and not only to Recommendations 5 and 10.

551. A requirement should be introduced to ensure observing AML/CFT measures in respect of branches and subsidiaries of the institution located in EU Member or European Economic Area.

552. A requirement should be introduced to the effect that where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries should be required to apply the higher standard, to the extent that local (i.e. host country) laws and regulations permit.

3.7.3 Compliance with Recommendations 15 and 22

	Rating	Summary of factors underlying rating
R.15	**PC**	• Lack of provision concerning timely access of the compliance officer to CDD and other relevant information

		• Lack of provision for compliance officers to be designated at managerial level. • No legal obligation introduced -in law, regulation or other enforceable means- for financial institutions to put in place comprehensive screening procedures to ensure high standards when hiring employees.
R.22	**LC**	• No requirement to ensure that foreign branches and subsidiaries observe AML/CFT measures consistent with the FATF Recommendations other than the requirements of R.5 and 10. • No requirement to apply the higher standard where requirements differ. • The requirement to ensure observing AML/CFT measures in respect of branches and subsidiaries is limited to institutions located in non-EU Member States (third countries).

Regulation, supervision, guidance, monitoring and sanctions

3.8 The Supervisory and Oversight System - Competent Authorities and SROs / Role, Functions, Duties and Powers (Including Sanctions) (R. 23, 29, 17 and 25)

3.8.1 Description and analysis

553. In the Slovak Republic the supervision over AML/CFT obligations is carried out by the FIU, the National Bank of Slovakia (hereinafter referred to as NBS), and by the Ministry of Finance (as a leading supervisor) in relation to gambling operators.

554. On 1st January 2006, the entire financial market supervision of the NBS covering banking, capital market, insurance and pension saving was integrated. As a part of the financial market supervision integration, the Financial Market Authority was dissolved by law and all its powers and responsibilities were transferred to the NBS. Since January 2006, the NBS has been the single supervisory authority over the financial market in the Slovak Republic. The general procedural rules followed by the NBS in supervising and regulating the financial market in the areas of banking, capital market, insurance and pension savings are laid down in Act No. 747/2004 Coll. on Supervision of the Financial Market and on amendments to certain laws as amended (hereinafter referred to as "FMS Act"). The supervisory and enforcement powers over AML/CFT issues are delegated to the NBS by Section 29 of the AML/CFT Act and are also endorsed in the FMS Act (Art. 1 para 2). The supervisory and regulatory powers defined in this law are exercised by the Financial Market Supervision Unit.

555. Market entry rules and licensing conditions for various market participants in all segments of the financial market are regulated in the following legislation respectively:

- the Act No 483/2001 Coll. On Banks,
- the Act No 566/2001 Coll. On Securities and Investment Services,
- Act No. 8/2008 Coll. on Insurance,
- Act No 186/2009 Coll. on Financial Intermediation and Financial Counselling,
- the Act No 492/2009 Coll. on payment services,
- the Act No 202/1995 Coll. Foreign Exchange Act.

556. Financial market entry is subjected to a licensing procedure, but one should also bear in mind Slovak membership of the EU, which allows the market to be entered by financial institutions

licensed in other EU Member States. In this process the respective supervisor (in this case the NBS) is formally notified by the home supervisory authority of the fact that a financial institution shall provide services on the territory of the Slovak Republic. Once a market participant enters the financial field, either licensed by the NBS or under the provision of the respective laws of the EU, the laws of the Slovak Republic provide for a set of measures for on-going supervision (i.e. Art. 50 of the Act on Banks).

557. According to paragraph 3 letter (a) of Article 1 of the FMS Act, the NBS supervises: *"banks, branch offices of foreign banks, securities dealers, branch offices of foreign securities dealers, stock exchanges, central depositories, asset management companies, branch offices of foreign asset management companies, mutual funds, foreign collective investment undertakings, insurance companies, reinsurance companies, branch offices of foreign insurance companies, branch offices of foreign reinsurance companies, branch offices of insurance companies from another state, branch offices of reinsurance companies from another state, pension asset management companies, pension funds, supplementary pension insurance companies, supplementary pension companies, supplementary pension funds, payment institutions, branch offices of foreign payment institutions, rating agencies, electronic money institutions, branch offices of foreign electronic money institutions, independent financial agents, financial advisers, the Deposit Protection Fund, the Investment Guarantee Fund, the Slovak Bureau of Insurers, consolidated groups, sub-consolidated groups, financial holding institutions, mixed financial holding companies, financial conglomerates, other persons, other property associations with a designated purpose and over groups of persons and property associations with a designated purpose, charged with obligations under separate laws in the area of banking, capital market, insurance business, pension insurance or pension schemes."*

558. Foreign exchange offices are also being supervised by the NBS, but on the grounds of paragraph 4 of Article 4 of the Foreign Exchange Act (202/1995).

559. Gambling operators (as defined in Section 2 letter (a) of the Gambling Act 171/2005) and internet casinos (as defined in Section 9 of the said Act) are supervised by, *inter alia*, the Ministry of Finance (please see R.24 for further details on the specifics of this supervisory architecture).

560. Under the provisions of the AML/CFT Act the supervision over AML/CFT issues is conducted by the FIU, the NBS, only over their supervised entities, as well as by the Ministry of Finance over the entities they supervise.

561. The NBS and the Ministry of Finance, before starting an on-site visit, inform the FIU of the business name, place of business or registered office, identification number and type of obliged entity which is to be controlled. After the control is completed the FIU shall be made aware of the results and measures taken. Should the NBS or the Ministry detect an unusual transaction or other facts that may be associated with money laundering or terrorist financing, the FIU shall be informed without undue delay. The authorities are also authorised to conduct on-sites together.

562. Obliged entities shall create appropriate conditions for the on-site inspectors and provide them with all necessary co-operation and refrain from any actions that may hamper the conduct of the on-site. The inspectors have access to written or electronic documents or equipment and records on data carriers, and are also authorised to make excerpts from them, notes and copies. Besides this the obliged entity shall provide the FIU, upon request, with information and written documents concerning the performance of obligations under Section 20 of the AML/CFT Act for a period of the past five years.

Authorities/SROs roles and duties & Structure and resources

Recommendation 23 (23.1, 23.2) (rated PC in the 3rd round MER)

Regulation and Supervision of Financial Institutions (c. 23.1); Designation of Competent Authority (c. 23.2)

563. The above mentioned new structure of the supervision over the Slovak financial market makes the FIU a central organ of supervision over AML/CFT issues. It is however paramount that the FIU is assisted by the NBS and the Ministry of Finance when it comes to the supervision over their entities in their respective fields. The co-operation between the FIU and the NBS is formalised additionally by the Memorandum of Understanding concluded in 2002 (which was the subject of analysis during the 3rd round mutual evaluation) and updated twice, in 2004 and 2006.

564. In 2007, the NBS performed a total of seven on-site inspections (also on the AML/CFT issues): one in a bank, three in securities dealer companies and three in asset management companies. No financial fines have been imposed, but corrective measures to improve the AML/CFT regime were introduced. In 2008 there were three on-site inspections in banks, one in an asset management company and five in securities dealers. No financial fine has been imposed either. From 2009 to September 2010 the NBS has performed one on-site visit in a bank, three in securities dealer companies and three on-site inspections in the insurance sector. No financial fines however have been imposed. On-site visits are conducted in a two-year-supervisory circle on the basis of the risk matrix and individual risk profile of each financial institution which is being kept by the NBS.

565. The NBS during their on-site visits to financial institutions use a "Procedure for the Anti-Money Laundering and Anti-Terrorist Financing Programme at banks and branches of foreign banks". The said document is quite comprehensive and covers broadly all relevant issues in AML/CFT regimes in financial institutions. It is worth pointing out that until the beginning of 2010 the NBS on-site visit did not include verifying compliance with EU Regulation 1781, and checking if the transfer messages are being screened against EU and UN sanctions lists. At this point the above mentioned Procedure does not include a detailed description of actions to be taken during an on-site visit by the NBS staff. This contingency lowers the effectiveness of the performed on-site visits.

566. The supervision on AML/CFT issues in the FX offices is being conducted by the FIU, though the NBS has supervisory powers over those institutions. The on-site visits conducted by the NBS do not however cover the AML/CFT compliance. It is worth mentioning that the NBS receives quarterly reports from each FX Office in Slovakia, stating, *inter alia*, the total turnover in foreign exchange, which is a good off-site instrument to detect any possible unexplained deviation from the former reports.

Recommendation 30 (all supervisory authorities) (rated PC in the 3rd round MER)

Adequacy of Resources (c. 30.1); Professional Standards and Integrity (c. 30.2); Adequate Training (c. 30.3)

567. The Financial Market Supervision Unit of the NBS employs almost 180 employees in three departments, where each department employs roughly 60 people. As it was provided by the NBS, a team of six to eight experts is focused on AML/CFT issues.

568. The Ministry of Finance, as the evaluation team was advised, designated three employees to conduct on-site visits in gabling operators, and four employees for the licensing proceedings.

569. The FIU has a department dedicated to supervise the obliged institutions on their observance of the AML/CFT Act. This Department employs seven people (including one head of the department) who

conduct the on-site visits. The staff consists mainly of long term employees (four of them are members of the staff for more than five years), and the new employees undergo a specific targeted training.

570. According to the data provided the NBS staff were trained in 2008 and 2010. The first training was focused on the changes made to the AML/CFT Act of the Slovak Republic, and the last one, conducted by the Czech Institute of Internal Audit, presented the experience and expertise of the Czech National Bank in this field. The number of trainings provided to the relevant employees in the NBS seems to be sufficient, but there was no training focuses on or even comprising the element of terrorist financing.

Authorities' powers and sanctions

Recommendation 29 (rated PC in the 3rd round MER)

Power for Supervisors to Monitor AML/CFT Requirement (c. 29.1); Authority to Conduct AML/CFT Inspections by Supervisors (c. 29.2); Power for Supervisors to Compel Production of Records (c. 29.3 & 29.3.1); Powers of Enforcement & Sanction (c. 29.4)

571. Section 29 of the AML/CFT Act reads:

"(1) Control of compliance to obligations of obliged entities laid down by this Act shall be performed by the Financial Intelligence Unit.

(2) Control of compliance to obligations may also be performed with a person who has ceased to be obliged entity to the extent of obligations that arose from law at the time of its being an obliged entity.

(3) Control of compliance to obligations laid down by this Act shall also be performed by the National Bank of Slovakia with obliged entities subject to supervision by the National Bank of Slovakia under a special regulation, and with obliged entities subject to surveillance by the Ministry under a special regulation, also by the Ministry.

(4) Prior to the commencement of a control under subsection 3, the National Bank of Slovakia and the Ministry shall notify the Financial Intelligence Unit of the business name, place of business or registered office, identification number and type of obliged entity under Section 5 which is to be controlled and after the control is completed, result of the control and measures taken. If a control conducted by the National Bank of Slovakia or the Ministry detects an unusual transaction or other facts that may be associated with legalisation or terrorist financing, the Financial Intelligence Unit shall be without undue delay informed about it.

(5) On the basis of mutual agreement, the Financial Intelligence Unit may control an obliged entity for compliance to obligations arising from this Act jointly with the National Bank of Slovakia or the Ministry."

572. As mentioned before, the FIU is placed at the centre of the Slovak AML/CFT regime, but the role of the NBS is also pivotal to the functioning of the entire system. The NBS follows its own procedures in a form of an on-site visit handbook for the inspectors. The said handbook covers all fields which one may deem important in the verification of the entities' internal AML/CFT regime. As the evaluation team was advised by the market participants, the on-sites conducted by the NBS are thorough.

573. The NBS as the supervisor, has enough and adequate powers to deal with its responsibilities. It was of concern whether the mechanisms in place in the Slovak Republic sufficiently impede any form of double sanctioning, as both the FIU and the NBS are allowed by law to sanction the financial institutions for breaches in AML/CFT regimes. As it was brought to the attention of the evaluators, the two bodies co-operate in this particular matter, i.e. by exchanging and negotiating plans for inspections, which is a clear obligation stated in paragraph 4 of Section 29 of the AML/CFT Act as described above.

574. Since there were no cases of double sanctioning and the co-operation between the two competent authorities seem to be on a good level, the evaluators assumed that the system in this matter works properly, though no sole body responsible for sanctioning has been explicitly named.

575. All of the institutions of the financial sector are under supervision for compliance with the AML/CFT issues, as Section 29 of the AML/CFT act relates to the obligations of respective market supervisors (the NBS and the MoF).

Effectiveness and efficiency (R. 23 [c. 23.1, c. 23.2]; R. 29, and R. 30 (all supervisors))

576. The procedure which is being used by the NBS during on-site visits is comprehensive, but does not provide for any detailed description on how the compliance with Regulation 1781 should be verified. It is important the NBS focuses more on the compliance with Regulation 1781 and screening of transaction messages against EU and UN sanctions lists, which has rarely been done. As the evaluation team was advised by the market participants, the on-site visits conducted by the NBS are thorough. The analysis of the said procedure supports this observation. It is also the impression of the team that the NBS' employees engaged in AML/CFT issues are competent

577. However, it is unclear how thorough and in depth the on-site inspections conducted by the MoF in gambling operators are, as the information received during the on-site visit's interviews were contradictory.

578. There should be more training for the NBS staff focusing on or comprising the subject of TF.

Recommendation 17 (rated PC in the 3rd round MER)

Availability of Effective, Proportionate & Dissuasive Sanctions (c. 17.1); Range of Sanctions—Scope and Proportionality (c. 17.4)

579. There is a vide variety of enforcement and corrective measures at the disposal of the NBS. The hierarchy of the penalties for banks is set out in paragraph 1 of Article 50 of the Act No. 483/2001 Coll. on Banks, allowing the NBS, depending on the seriousness, scope, duration, consequences, and nature of detected shortcomings impose sanctions, corrective measures and fines. Enforcement and corrective measures directed at other financial market participants are set out in paragraph 1 of Article 144 of the Act No. 566/2001 Coll. on Securities and Investment Services, paragraph 1 of Article 67 of the Act No. 8/2008 Coll. on Insurance, paragraph 2 of Article 78 of the Act No. 492/2009 Coll. on Payment Services and paragraph 2 of Article 86 of the same act. Articles 24 and 24a of the FX Act provides for the details for the conduct of FX controls and the way how corrective measures (in case of irregularities are detected) are to be imposed.

580. The above mentioned legal provisions have been constructed using roughly the same wording, which, in the opinion of the evaluators, allows applying the sanctions and actions stated in them also to any violations of the AML/CFT Act. For example, Article 50 of the Act on Banks allows the NBS, depending on the seriousness, scope, duration, consequences, and nature of detected shortcomings, to take measures stated in this article. Article 50 reads: *"If the National Bank of Slovakia finds any shortcomings in the operations of a bank or branch office of a foreign bank consisting in a failure to comply with the terms specified in its bank license (…) or a violations or circumvention of other provisions of this Act, legally binding Acts of the European Communities and the European Union pertaining to banking activities, separate regulations, or generally binding regulations governing the conduct of banking operations the National Bank of Slovakia may, depending on the seriousness, scope, duration, consequences, and nature of detected shortcomings:…"* A footnote to this article clearly states that one of the act sanctionable under this provision in also the AML/CFT Act. Since the 3rd round evaluation the NBS has not imposed any fines based on this article for any breach of the AML/CFT Act. As stated in paragraphs 614-618

above the evaluation team is convinced that the existing co-operation mechanisms between the FIU and the NBS are sufficient to deal with the potential issue of double sanctioning, though there is no direct provision in the Slovak legislation, which would designate a sole authority responsible for imposing fines.

581. The AML/CFT Act regulates (in Part 6) administrative offences and measures. It is the understanding of the evaluators that the measures described in part 6 of the AML/CFT Act can be fully applied to situation stated therein by the FIU. Should the NBS wish to sanction a financial institution for the breach of AML/CFT Act this may be done (as there is no explicit legal impediment to do so), but on the grounds of the provisions of special acts, as stated above.

582. Under the AML/CFT Act the FIU:

"(…) shall impose on a legal entity and a natural person– entrepreneur a fine of up to:

a) €165,969 for failure or breach to comply with any of the obligations laid down by this Act under Section 10 subsection 1 to 4, 6 to 11, Section 11 subsection 3, Sections 12, Section 14 to 17 and Section 20,

b) €99,581 for failure or breach to comply with any of the obligations laid down by this Act under Section 18 subsection 1, Section 19 subsection 2 to 4, Section 21, Section 24 subsection 1 to 4, Section 30 subsection 1 and 2;

c) €66,387 for failure or breach to comply with obligation laid down by this Act unless it is referred to in letters a) or b)."

"The Financial Intelligence Unit shall impose on a legal entity and a natural person– entrepreneur a fine of up to €331,939:

a) for an administrative offence under subsection 1, letter a) and b) provided the obligation shall not be complied or shall be breached for 12 consecutive months,

b) if an administrative offence under subsection 1 shall hamper or substantially impede seizure of proceeds of criminal activity,

c) which repeatedly breaches an obligation for which a fine under subsection 1 has been imposed in three years preceding."

583. Apart from other factors, the seriousness, duration and consequences of the unlawful conduct has to be taken into consideration by the FIU when imposing the said penalties. Furthermore, should the obliged entity for more than 12 consecutive months or repeatedly not complies with or breaches obligations laid down in the AML/CFT Act, the FIU may initiate, with the proper authority, the conduct to revoke the license. All breaches of the AML/CFT Act, or other forms of failure to comply with the said provisions are sanctionable. Article 33 contains a catalogue of breaches, which are subject to a specific amount of fine, and the general clause of section 1 letter (c) of this article deals with breaches of provisions of AML/CFT Act that are not referred to in other articles of part 6 of the Act.

584. The range of sanctions that may be imposed by the NBS and the FIU is wide. The evaluators believe that the catalogues provided for in the mentioned provision of special laws, as well as the catalogues in the AML/CFT Act paint a picture of effective, proportionate and dissuasive sanctions available to the appropriate institutions. There is, however, an outstanding issue of the ability to use those sanctions, as described below.

Designation of Authority to Impose Sanctions (c. 17.2)

585. As discussed previously under R.29 both the FIU and the NBS are allowed by law to sanction the financial institutions for breach in AML/CFT regimes, however their catalogue of sanctions differ, which was discussed above. No sole body has been named by the law, neither is there any legal impediment for the NBS to sanction breaches of the AML/CFT Act. The co-operation between the two authorities seems to be sufficient.

586. The co-operation between the FIU and the MoF also seem to be adequate. It may, however, be considered a big disadvantage that the two bodies do not exchange inspection plans, which may negatively impact the effectiveness of actions undertaken by each of the authority. This is especially important in the light of the fact that both the MoF and the FIU may sanction gambling operators on their breaches of AML/CFT Act. But as in the situation described above in relation to the NBS and the FIU, the MoF may sanction the supervised entities under the provisions of Section 54 of the Gambling Act. The FIU on the other hand has at their discretion all the sanctions set out in the AML/CFT Act.

587. The evaluators were advised that the NBS and the MoF forward each case of breach of AML/CFT Act to the FIU in order for them to apply proper sanctions.

588. The FIU and the NBS should, however, consider whether it would be advisable to clearly state the division of competences in sanctioning in the existing MoU.

Ability to Sanction Directors and Senior Management of Financial Institutions (c. 17.3)

589. The FIU may only sanction legal entities, and the only exception is the ability to sanction tipping off under Section 18 of the AML/CFT Act. Any natural person may, however, be sanctioned by the NBS. As it was stated above, there is a practice of both the NBS and the MoF to forward any cases of violations of the AML/CFT Act directly to the FIU. Hence the FIU is obliged to impose proper sanction on the grounds of the mentioned Act. However, only the direct addressees of the provisions of special laws (so the NBS and the MoF) may use the range of penalties stated therein. It is, therefore, impossible for the FIU to sanction the directors and senior management of financial institutions except for the cases stated in Section 18. In conclusion, it must be stated that the provisions of special laws cannot be taken into account when evaluating the compliance of Slovak law with Recommendation 17, as they cannot be used by the FIU, which was practically named as the sole institution to impose penalties.

590. The range of sanctions available should include the power to impose disciplinary and financial sanctions and the power to withdraw, restrict and suspend the financial institution's license where applicable. As mentioned the catalogue provided in the special laws is broad enough to encompass the requirement of criterion 17.4. It should be dully noted that the FIU has the power to apply for the revocation of license, and can impose financial sanctions on legal persons, but may not apply any form of disciplinary actions or financial sanctions against directors and senior management. Though those powers are present in the legal system, they cannot be used in practice by the authority designated to impose fines and penalties. This is why the evaluators see as a deficiency the fact that although the range of sanctions available is broadly in line with criterion 17.4 it may not be used by the FIU, which in effect leads to a conclusion that directors and senior management of financial institutions cannot be sanctioned for violations of the AML/CFT Act.

Market entry

Recommendation 23 (rated LC in the 3rd round MER)

Recommendation 23 (c. 23.3, c. 23.3.1, c. 23.5, c. 23.7, licensing/registration elements only)

Prevention of Criminals from Controlling Institutions, Fit and Proper Criteria (c. 23.3 & 23.3.1)

591. Financial institutions, when entering the market, are subjected to a licensing procedure. The conditions required to grant the license must be maintained throughout the future activity of the institution. Strict legal provisions allow for the transparency of the future shareholders. The provisions regarding fit and proper testing and issues connected with licensing of the financial market participants can be found in Articles 3, 7-9 and 28 of the Act on Banks, in Articles 8, 54-56,

59 and 70 of the Act on Securities and Investment Services and in Articles 4-9, 12 and 44 of the Act on Insurance.

592. Article 3 of the Act on Banks stipulates the activities that require a banking license. Before, however, granting such a license, the institution is subject to proceedings in which it must provide full and comprehensive information, also on its ownership structure. When the bank is granted a license, any changes in the ownership structure above the threshold stipulated in Article 28 of the Act on Banks require the approval of the NBS. The lack of such approval renders the contract null and void.

593. Article 8 letter (b) of the Act on Securities and Investment Services provides a definition of a trustworthy person, and such person only may be a senior manager or a person responsible for the compliance function, risk management function or internal audit function. As in the Act of Banks, further provisions establish high standards on information to be provided before the license is granted. The obligation of a prior approval for the acquisition of shares is present as well.

594. The same as above can be said for the insurance companies sector, as mentioned in the Act on Insurance in Art. 4-9, 12 and 44.

Licensing or Registration of Value Transfer/Exchange Services (c. 23.5)

595. The system for the licensing and registration of value transfers and exchange services can be found in Articles 64-67, 81-83 of the Act on Payment Services and in Article 6 of the Foreign Exchange Act. The Act on Payment Services is the Slovak implementation of the PSD.

596. Before granting a license for a payment service provider the NBS must be satisfied i.e. of:

- the fact that the minimum paid-up contribution to the payment institution's registered capital was made;
- there is a transparent, credible and legal origin of the monetary contribution to registered capital;
- the suitability of persons with qualifying participation in the payment institution and transparency of those persons' relationships with other persons, particularly transparency of their holdings in registered capital and voting rights of other legal entities;
- professional competence and credibility of natural persons nominated as members of the statutory body, confidential clerk, members of the board of supervisors, managers and head of an internal control body.

597. There is an obligation for prior approval to acquire the shares of such a company, with consequences to the lack of such approval as stated above.

598. To be granted a foreign exchange license a natural person must be a trustworthy person, be at least 18 years old, be eligible for legal acts, and have a full secondary education. Trustworthiness is defined for the purposes of this Act also in Article 6.

599. The requirements set out in the Slovak law seem to generally mitigate the shortcomings pointed out in the 3rd round MER.

Licensing of other Financial Institutions (c. 23.7)

600. There are no other financial institutions not mentioned in criterion 23.4. operating on the territory of the Slovak Republic

On-going supervision and monitoring

Recommendation 23 & 32 (c. 23.4, c. 23.6, c. 23.7, supervision/oversight elements only & c. 32.2d)

Application of Prudential Regulations to AML/CFT (c. 23.4); Statistics on On-Site Examinations (c. 32.2(d))

601. As was mentioned earlier in this report, the NBS conducts on-site inspections on AML/CFT issues, designating the entities to be supervised by using the risk matrix. The supervisory cycle is two years. For statistics on supervision please see paragraph 607 of this report.

602. As the evaluation team was advised by the market participants the level of thoroughness of the on-site inspections is sufficient, and actions taken by the NBS in accordance with proper legal provision afterwards are focused on mitigating the risks arising from the found shortcomings.

603. The scope of on-site inspections conducted by the NBS seems to be generally broad, but as mentioned previously, the examination of EU Regulation 1781 compliance is not frequent enough.

604. The NBS uses a risk matrix, and a risk-based approach towards the supervisory obligations in relation to AML/CFT. Fit and proper testing for high ranking employees of the supervised entities and the thorough examination of the ownership structure is also used to ensure compliance with AML/CFT provisions. The evaluation team considers that criterion 23.4 is satisfied at present.

Monitoring and Supervision of Value Transfer/Exchange Services (c. 23.6)

605. The foreign exchange offices are being supervised on AML/CFT issues by the NBS. As mentioned previously the off-site monitoring in AML/CFT issues may be done by the virtue of the quarterly reports received by the NBS from the exchange offices. The supervision in this field is, however, conducted by the FIU over both exchange offices and value transfer services.

Supervision of other Financial Institutions (c. 23.7)

606. There are no other financial institutions that are not mentioned in criterion 23.4 operating on the territory of the Slovak Republic

Statistics on On-Site Examinations (c. 32.2(d), all supervisors)

607. For statistics on supervision please see under Recommendation 23 (23.1, 23.2) above.

Statistics on Formal Requests for Assistance (c. 32.2(d), all supervisors)

608. During the on-site visit the evaluation team was not given any statistics on international co-operation and requests for assistance from foreign supervisory authorities. As the Slovak authorities explained the co-operation is taking place in practice, however, the statistics are not kept.

Effectiveness and efficiency (market entry [c. 23.3, c. 23.3.1, c. 23.5, c. 23.7]; on-going supervision and monitoring [c. 23.4, c. 23.6, c. 23.7], c. 32.2d], sanctions [c. 17.1-17.3])

609. The Slovak legal system seems to be generally in line with EU regulations on financial institutions. The provisions of law on market entry and supervision (on-site as well as off-site) are comprehensive in accordance with the FATF standards, and the team was not informed of any contingency which may hamper its effectiveness. It is, however, paramount to stress that the overall effectiveness of the system may be weakened by the level of on-site inspections conducted by the MoF.

610. The Slovak law does provide for a full scope of sanctions. However, as the Slovak authorities have clearly stated that the sole body responsible for sanctioning is the FIU; there are no clear legal provisions on this matter, which is why it may be helpful to specify this at least by a way of internal MoU.

611. The consequence of the fact that the NBS does not sanction on AML/CFT matters is that the provisions of special laws cannot be taken into account when evaluating the compliance of Slovak law with R.17, as they cannot be used by the FIU, and can be used only by the NBS. This fact influences the effectiveness to a major degree.

612. The overall picture of the Slovak system with the FIU at the centre, arising for the assessment of the above mentioned recommendations is pretty much clouded by the fact that the FIU cannot use a wide and dissuasive range of sanctions provided in the special laws, and that the NBS does not do so. The process of granting a license and ongoing supervision (on-site and off-site) is in place and can be deemed effective. As the analysis above indicates the process of sanctioning the breaches of AML/CFT Act is not complete, and falls short of FATF standards.

Guidelines

Recommendation 25 (c. 25.1 – guidance for financial institutions other than feedback on STRs)

613. Slovakia was rated "*Non-Compliant*" with regard to R. 25 in the 3rd round MER. The report noted the lack of guidance on both ML and TF related issues to financial institutions and DNFBPs to assist their implementation of the reporting duties on AML/CFT. Therefore, it is recommended that the Slovakian authorities should establish co-ordinated and consistent sector-specific guidelines on AML/CFT issues to assist financial institutions and DNFBPs and should also provide appropriate feedback in line with the FATF Best Practices Guidelines.

614. The NBS in co-operation with the FIU and the Ministry of Finance issued Methodological guidance of the Financial Market Supervision Unit of the National Bank of Slovakia No. 4/2009 for protection of a bank and branch office of a foreign bank against money laundering and terrorist financing. However, guidelines of this kind have not been developed for other financial institutions or DNFBPs.

615. In an Annex to the mentioned Methodological guidance, a set of indicators for recognising unusual transactions was developed. These indicators relates to money laundering only, but not to terrorism financing. The AML/CFT Act, in its provisions on reporting unusual transactions, also contains some general indicators for recognising ML.

616. Apart from the mentioned document which is only addressed to banks and a very comprehensive one, the FIU has issued some guidelines on it's official web site which are very specific in their nature. Evaluators have been provided with "Guidelines for leasing companies" which describe some fraudulent actions related to interconnected companies, "Guidelines for credit institutions" related to misuse of EFT POS terminals, to tax criminal offences, to procedure upon the discovery of case of phishing and pharming, to false identification documents, and to potential way of terrorist financing connected with one legal entity from United Arab Emirates. "Guidelines for advocates related to misuse of client account" has been provided as well as guidelines regarding record-keeping, CDD measures for entrepreneurs that carry transactions in cash exceeding €15,000, refusal to establish or termination of relationship or transaction, FATF statements, and detection of beneficial owner and PEP, all addressed to all reporting entities.

617. When it comes to possible terrorism financing, indicators set out in the AML/CFT Act concentrate on possible suspicious transactions which are related to international sanctions. Methodological guidance also contains a section on terrorism financing, but again it concentrate only on international sanctions. Some inconsistencies and outdated information is presented here because some of the entities mentioned in this respect do not exist anymore (e.g. reference to Yugoslavia). No other indicators for recognising possible terrorist financing have been provided to financial institutions or DNFBP.

618. Beyond the recommendations on how to organise the UTR reporting process (in part F - identification, delaying and reporting of an unusual transaction) the Methodological guidance encompasses also other areas, which have to be addressed to establish an effective preventive regime, which would be in line with legal obligations introduced by the AML/CFT Act, such as:

1. The concept and basic principles of protection of a bank against ML and TF;
2. Employees responsible for the implementation of tasks of protection against ML and TF;
3. Program of bank activities against ML and TF;
4. Familiarisation with the matter, education of employees, information system;
5. Identification and client's acceptance, client's risk profile, CDD, SCDD, ECDD; third parties reliance;

G. Measures against TF;
H. Preservation of data and documentation;
I. Security of the system and performance of internal control.

619. It has to be noted that the Methodological guidance deals in details with the whole range of issues with regard to organisational and other measures needed for effective implementation of the AML/CFT Act, but ML and TF techniques, methods, trends and typologies are not described therein.

620. The Slovak FIU co-operates with self-regulatory organisations and associations of obliged entities with regard to outstanding issues on implementation of the AML/CFT Act in particular. It addressed in writing all the associations, chambers and professions of the obliged entities to notify them about the establishment of its website. Obliged entities met on-site were aware of the existence of the FIU's website. Almost all of them reported that guidelines could be found on the mentioned website. The FIU has a link on the website to the Ministry of Interior. It seems well organised and contains following topics: organisational structure of the FIU with descriptions of competencies of different departments, list of reporting entities according to the AML/CFT Act, obligations of reporting entities with sanctions for non-compliance, legislation in force, annual report of the FIU, list of equivalent countries and territories according to EU legislation, guidelines for proper application of the provisions of the AML/CFT Law in practice,, MONEYVAL and FATF public statements, reporting forms and contacts. The FIU provides on its website some sanitised cases, which may be useful when comes to reporting of STRs.

621. The FIU has requested from abovementioned organisations and profession associations to provide e-mail contacts, to which it regularly sends the necessary information on how to properly apply the AML/CFT Act in daily practice, and also other important information relating to ML/TF. Those organisations will subsequently inform their members whereby an effective communication between the FIU and reporting entities is enabled. The obliged entities are systematically informed also using other ways, particularly through training courses conducted by the FIU as well as within the frame of performance of supervisory inspection (on-site control) in a concrete obliged entity.

622. The Slovak authorities reported that the FIU's police performed in total 27 trainings for obliged entities and their professional organisations in 2009 in order to eliminate application discrepancies stemming from interpretation of the new AML/CFT Act.

Table 14: The number of trainings performed by the FIU officials in 2009

Obliged entity	Number of trainings
Credit institution - bank	1
Insurance companies	4
Finance lease - leasing companies	2
Accountant and Tax advisor	1
Securities dealer association	1
Real Estate Agency	3
National Association of Real Estate Agencies	2
Export-Import Bank of the Slovak Republic	1
Postal undertaking	1
Gambling game operators	5
Trading in receivables	3
Court distrainer	1
Notary's Chamber	1
Service providers of property or management of company	1
Total	**27**

623. The evaluators welcome the efforts made by the FIU in its outreach activities to financial sector and DNFBPs. It is noted that obliged entities are aware of their obligations in respect to AML/CFT but still in most of the cases this awareness raising is in its initial phases. All the reporting entities, especially DNFBP, should receive more guidance on risks on ML and TF, methods and techniques used for ML and TF and on measures that can be undertaken to mitigate those risks. The FIU is encouraged to continue with its activities in this sense. Concerns regarding resources given to the FIU to undertake these tasks, have to be repeated and emphasised once more.

624. Besides the FIU, the NBS has also taken some measures in providing guidance to obliged entities. These activities, which are limited to the banking sector, should be extended to all other sectors, subject to the supervisory activities of the NBS.

Effectiveness and efficiency (R. 25)

625. The guidelines provided by the NBS for banks are comprehensive The Slovak authorities should, however, provide financial institutions other than banks with sector specific guidelines.

3.8.2 Recommendations and comments

Recommendation 23

626. It appears that the supervisory framework has been strengthened by the Slovak authorities since the 3rd round evaluation and is now broadly in line with the FATF Recommendations.

627. When it comes to the effectiveness, it is still, however, a concern of the evaluation team that the level of on-site inspections conducted by the MoF may not be sufficient enough.

628. There should be more training for the NBS staff focusing on or comprising the subject of TF.

629. It should be further elaborated by the NBS whether the on-site inspections procedure should also include a detailed description of supervisory measures to be taken during an on-site visit by the NBS staff, as the lack of those provisions may be deemed a contingency, lowering the effectiveness of the performed on-site visits.

Recommendation 17

630. The scope of the sanctions and preventive measures in place is broad enough.

631. It is, however, an issue that the FIU cannot use a wide and dissuasive range of sanctions provided in the special laws, which makes the Slovak legal system fall short of the FATF standards. Therefore, Slovak authorities should, therefore, take necessary steps with a view to ensuring the FIU uses a wide and dissuasive range of sanctions provided for in the special laws.

632. The potential double sanctioning may still be considered an issue, and that is why the Slovak authorities are advised to consider whether the detailed provisions on avoiding double sanctioning should be clearly stated in the MoU between the NBS and the FIU.

633. It is considered a big disadvantage that the FIU and the MoF do not exchange inspection plans, which may in impact the effectiveness of actions undertaken by each of the authority.

634. Although the range of sanctions available is broadly in line with criterion 17.4, these may not be used by the FIU, which in effect leads to a conclusion that the directors and senior management of financial institutions cannot be sanctioned for AML/CFT Act violations. This issue should be clearly addressed by the Slovak authorities.

Recommendation 25(c. 25.1 [Financial institutions])

635. Guidelines on implementing AML/CFT measures are given to the banks, insurance and leasing companies, together with some guidelines regarding CDD, record-keeping and FATF statements that are addressed to all reporting entities. Some guidelines are given through the website of the FIU and in direct contact with reporting entities. Still, authorities should focus more on this issue due to the fact that not all the sectors have received specific guidance and that the guidelines already issued, except for the banking sector, are very brief and in most of the cases relate to very specific cases that the FIU experienced in its work, thus having limited space to be used. Therefore, Slovak authorities should issue guidelines to financial market participants other than banks, and the FX offices as well.

Recommendation 29

636. The NBS as the supervisor has enough and adequate powers to deal with its responsibilities. The NBS on-site visits are thorough and deal generally with all important parts of the financial institutions AML/CFT regimes, notwithstanding the deficiencies in the procedure stated above. There is, however, a need to place more emphasis on verifying compliance with SR.VII during on-site visits.

637. It is unclear how thorough and in depth the on-site inspections conducted by the MoF are in respect to gambling operators. Otherwise it seems the MoF is properly equipped with the legal duties and powers to deal with the tasks assigned to them in the AML/CFT regime of Slovakia. More emphasis should, however, be placed on a proper number of employees to deal with the supervisions.

638. The FIU has proper resources to deal with the supervisory responsibilities in the AML/CFT field, especially the on-site supervision, when it comes to financial institutions (setting aside the DNFBPs

sector). The level of thoroughness, judging from the interviews conducted during the evaluation on-site visit, is sufficient.

639. The NBS, on the grounds of Article 2 (7) of the FMS ACT, is authorised to compel production of any information that can be relevant. The evaluation team was advised during the on-site visit that this power is used widely and the financial institutions are aware of their obligations, and penalties which may be imposed for non-compliance with this specific provision of law. The MoF is also authorised to compel production of: "*of originals of documents in a specified period, other papers, statements and information including technical data mediums necessary for the exercise of supervision*" according to part. 1 letter (b) of Section 11 of the Gambling Act. This power is, however, limited only to a supervision, which from the context of this act could be interpreted as an on-site inspection.

640. The range of sanctions (already discussed in this report) which can be imposed on the institutions and over their directors and senior managers is broad enough. It is worth to stress again, that the power to impose sanctions on physical persons can be exercised only by the NBS, and not the FIU and the MoF, with the exceptions stated in paragraph 632 above.

Recommendation 30 (all supervisory authorities)

641. The NBS has sufficient resources, and the employees seem to be well trained. It is, however, important to provide TF trainings to employees engaged in AML/CFT issues.

642. The FIU staff designated to conduct on-site visits is also well trained and experienced, and the evaluators believe that in this particular manner the FIU is also properly staffed.

643. It is of concern that the MoF is not sufficiently staffed to deal with the responsibilities of conducting on-site inspections.

Recommendation 32

644. During the on-site visit the evaluation team was not given any statistics on international co-operation and requests for assistance from foreign supervisory authorities. Other statistics provided by the NBS were comprehensive and detailed enough. The evaluation team was not presented, however, with detailed and comprehensive statistics from the MoF, although the general idea of the actions taken by this body might have been inferred from the on-site visit interview.

645. Setting aside these, the statistics provided by the other relevant Slovak authorities on the on-site visits were sufficient and comprehensive.

3.8.3 Compliance with Recommendations 23, 29, 17 & 25

	Rating	Summary of factors relevant to s.3.10. underlying overall rating
R.17	**PC**	• Sanctions are mostly not applicable to directors and senior management by the FIU and MoF. • Full range of sanctions is not available for the use of the FIU. • No provisions available to avoid double sanctioning.
R.23	**LC**	• The level of on-site inspections conducted by the MoF is not sufficient enough.
R.25	**PC**	• No sector specific guidelines to cover financial market participants other than banks. (25.1)

R.29	**LC**	• Not enough focus is placed in the scope of the on-site visits on issues of SR.VII.

4 PREVENTIVE MEASURES – DESIGNATED NON FINANCIAL BUSINESSES AND PROFESSIONS

Generally

646. A description of the DNFBPs operating in Slovakia is set out in sections 1.3 and 4 of the 3rd round MER.

647. In Slovakia, all DNFBPs are covered by the AML/CFT Act as obliged entities and are therefore subject to the same CDD and record-keeping requirements as financial institutions. The main DNFBPs in the Slovak AML/CFT Act (Section 5) are real estate dealers, gambling game operators, precious metals or gemstones dealers, lawyers, notaries, auditors, accountants and tax advisors. The AML/CFT Act, in addition to those DNFBPs defined in the FATF Glossary, include service providers of property management or company service providers, legal entities or natural persons authorised to provide services of organisational and economic advisor, the services of public carriers and messengers or forwarding services, auction hall operators, legal entities or natural persons authorised to trade in works of art, collector's items, antiques, cultural monuments, items of cultural heritage and pawnshop operators in the obliged DNFBP categories. The Slovak Law still does not allow the creation of trusts.

4.1 Customer due diligence and record-keeping (R.12)

(Applying R.5 to R.10)

4.1.1 Description and analysis

648. As laid out above, DNFBPs are subject to the same CDD and record-keeping requirements as financial institutions. Therefore, the same concerns in the implementation of Recommendations 5 to 10 apply equally to DNFBPs. For details see section 3 of the Report. The following remarks only refer to topics that differ from the description and analysis made in section 3.

Recommendation 12 (rated NC in the 3rd round MER)

Applying Recommendation 5(c. 12.1)

Casinos (Internet casinos / Land based casinos)

649. Section 10 of the AML/CFT Act requires all obliged entities to perform CDD when their customers carry out a transaction the amount of which reaches at least €2,000. This particular provision does not state that this threshold applies also regardless of whether the transaction is carried out in a single operation or in several linked operations. This is true only for transaction of an amount over €15,000. It is understood that the transaction in question related to the buying or selling of gambling chips, but the scope of the provision is broad.

650. As at the time of on-site visit, there were three companies in the Slovak Republic (with nine gambling places), which were authorised for operation of casinos. The number of subsidiaries of these three companies was eight as at 30 June 2010. Section 9 of the Gambling Act allows the operation of an internet casino, and it is the understanding of the evaluators that all measures applied to land based casinos also apply to internet casinos.

Real estate agents

651. The AML/CFT Act defines legal and natural persons that are authorised to mediate sale, rent or purchase of real estate as obliged entities. Though the Act does not specify the cases when they apply CDD requirements, it can be interpreted that those persons should take CDD measures when they involved in transaction for a client concerning buying and selling of a real estate as required under R.12.

652. Although the legal framework for real estate agents to apply CDD measures exists, it is the evaluators' distinct feeling, based on interviews conducted during the on-site visit, that those measures are not being applied in practice. The awareness in this sector may be described as less than adequate, and the overall effectiveness is seriously hampered.

Dealers in precious metals and dealers in precious stones

653. As casinos, dealers in precious metals and dealers in precious stones are also obliged to perform CDD when their customers carry out a transaction the amount of which reaches at least €2,000. The threshold is well below the threshold determined under R.12 (USD/€15,000); this is, however, in line with the requirement.

Lawyers, notaries and other independent legal professionals and accountants

654. As noted above, lawyers and notaries, as the obliged entities under the AML/CFT Act, are also obliged to apply CDD measures in line with the requirements of R.12. They are subject to CDD obligations when they are providing customers with services related to the following activities:

- buying and selling of real estate or ownership interests in a company;
- management or safekeeping of funds, securities or other property;
- opening or management of an account with a bank or a foreign bank branch or of a securities account;
- establishment, operation or management of a company, an association of natural persons or legal entities, a special-purpose corporation or of another legal entity.

655. The evaluators, however, believe that such obligations are not being fulfilled at all in practice and, this belief arises from the interviews held during the on-site visit and the opinions presented by the interlocutors from this sector. The interlocutors the legal professional seemed to lack proper training, guidelines, and any detailed knowledge whatsoever about the AML/CFT issues. Furthermore, the evaluation team came to the conclusion that there appears to be no contact between the FIU and legal professionals, and as far as the FIU is concerned the co-operation is rather poor. The FIU, however, stressed that they do send feedback to obliged entities other then those from the financial sector every half year. The co-operation of the Slovak FIU with DNFBPs is realised, according to the FIU, via regular meetings with associations of DNFBPs, and other information is provided via the e-mail addresses of the associations which are expected to distribute them to their members.

656. There is still an urgent need for a very broad outreach to this sector. As a general rule, the deficiencies stated under the revision of R.5 in this report apply also to R.12.

657. The external auditors on the other hand are fully versed in their obligations. The identification of the client is complete, and compliant with the FATF standards. The awareness in this particular sector can be deemed high and the effectiveness of implementation sufficient.

Trust and company service providers

658. As noted above, the activities of trust and company service providers are not allowed in Slovakia. Therefore, the AML/CFT Act does not determine respective requirements.

659. It should be noted that subsection (4) of Section 10 of the AML/CFT Act allows all obliged entities, including DNFBPs, to determine the extent of CDD measures on a risk-sensitive basis depending on the type of customer, the type of transaction, the business relationship or a particular transaction.

Applying Recommendations 6, 8, 9[16] and 11(c. 12.2)

660. The AML/CFT Act applies to DNFBPs the same way as to financial institutions and the same strengths and weakness in relation to Recommendations 6, 8 and 11 are present (see section 3.2. of the Report)

661. Although the legal framework is in place to oblige the DNFBPs to fulfil the obligations set out in Recommendation 6, 8, 9 and 11 the effectiveness of such mechanisms is extremely poor. From the interviews of the on-site visit the evaluators received the impression that none of the legal professionals, real estate agents or accountants seemed to be aware of the nature of their obligations. They were also not aware of some of the institutions (like PEPs) introduced in the AML/CFT Act, which means they do not use it in the day-to-day practice. The issue of beneficial owner was also not meet with recognition in most of the representatives of this sector.

662. It is of significant importance to provide extensive outreach to this sector on their obligations. The low number of STRs, in the opinion of the evaluators, may also be treated as a proof of inadequate implementation of FATF standards, because the sheer lack of knowledge translated directly into lack of reports.

663. On the other hand, the external auditors seem to be generally very much aware of their obligations, and volunteered information on how each measure set out in FATF Recommendations is being fulfilled.

664. The evaluation team notes that the FIU has provided guidelines to gambling operators, entrepreneurs dealing with cash exceeding the value of €15.000, auditors, accounts, executors, real-estate agents and advocates. As mentioned above the level of awareness is, however, still poor.

Applying Recommendation 10

665. The evaluation team is satisfied that the provisions of the AML/CFT Act are being effectively observed in the matter of record-keeping. It is, however, worth mentioning that in some cases (notaries and lawyers) this is only due to the fact that provisions of sector specific laws governing their activities provide for the same or an even longer period of record-keeping obligations, as the evaluation team was advised by the interlocutors during the on-site visit. The respective legal provisions indeed do require DNFBPs to keep the records. This is the case for example in relation to executors (the obligation is set out in Execution Act No. 233/1995 Coll.), notaries (The obligation is set out in Notarial Act No. 323/1992 Coll. which requires notaries to keep original records for 100 years) and accountants (the obligation is set out in Act No. 431/2002 Coll. on accountancy).

[16] Criterion 12.2 refers to Recommendation 6 and Recommendations 8-11. Recommendation 9 was rated as "Largely compliant" in the 3rd round MER. As this Recommendation neither constitutes key or core Recommendation, it has not been re-assessed during the 4th round evaluation. In accordance with the considerations in the note to assessors in MONEYVAL's 4th Cycle of Evaluations the evaluators of this round relied on the information existing in the 3rd round MER so far as possible. As the new AML/CFT Act includes a parallel legal framework for this Recommendation, which has not been changed, the evaluators have relied on the information in the 3rd round MER so far as possible for this element of their re-assessment, but they have not taken into consideration in the rating for Recommendation 12.

Effectiveness and efficiency

666. An urgent need for an awareness raising programme to promote effective compliance for DNFBP sector was identified as one of the deficiencies regarding R.12 in the 3rd round MER. The evaluators of this round have noticed that no concrete and meaningful steps have been taken to rectify this deficiency since the adoption of the 3rd round MER.

667. Setting aside the external auditors, there is no effective implementation of this Recommendation whatsoever. Generally, the DNFBP sector is not aware at all of their obligations arising from the AML/CFT Act, and their knowledge on the potential factors triggering STR reporting is also less than adequate.

4.1.2 Recommendations and comments

668. There is an urgent need for an extensive outreach to this sector to make them aware of AML/CFT issues and their obligations under the AML/CFT Act, and Recommendations 5, 6, 8, and 11.

Recommendation 5

669. Actions should be taken with immediate effect to make the real estate agents, lawyers, notaries and other independent legal professionals and accountants fully aware of their obligations under the AML/CFT Act, and to apply them in practice. Section 5(1)(h) of the AML/CFT Act should be amended so as to add: "when undertaking their professional activities, including when acting as in item (j) of this paragraph".

Recommendation 6

670. It is of great concern that the obligations regarding PEPs are not complied with at all by this sector. This must be addressed by the Slovak authorities, mainly by providing more extensive outreach to this sector.

Recommendation 8

671. Though the legal framework applies to all of the obliged entities it is the evaluators' opinion that the DNFBP sector does not apply it in practice.

Recommendation 9

672. There is hardly any recognition in the DNFBP sector of the obligations set out in R.9 and implemented in the Slovak Law, as they apply to their activities.

Recommendation 10

673. In the case of notaries and lawyers, the record-keeping obligations are met mainly due to the fact those provisions observe other laws relating strictly to their activity, and not the AML/CFT Act. This should be taken into account by the Slovak authorities in the awareness raising programmes designed for these professionals.

Recommendation 11

674. The issue of lack of awareness in the DNFBP sector is especially vividly seen, when it comes to paying attention to unusual and complex transactions. The sector representatives – with few notable

exceptions – could not actually give any meaningful information which would indicate that the conditions of R.11 are understood and applied. This should be of special interest of the Slovak authorities.

4.1.3 Compliance with Recommendation 12

	Rating	Summary of factors relevant to s.4.1 underlying overall rating
R.12	**PC**	• The same formal shortcomings under R.5, 6, 8, 10 and 11 equally apply to DNFBPs. • The awareness of the legal obligations under the AML/CFT Act especially under R.5, 6, 8 and 11 is insufficient. • The said obligations are not at all being used by most of the DNFBP in practice. • The outreach to this sector is insufficient. • The threshold of €2000 does not apply regardless whether the transaction is carried out in a single operation or in several linked operations. **Recommendation 5** • The real estate agents, lawyers, notaries and other independent legal professionals and accountants have insufficient knowledge of any CDD requirements. **Recommendation 6** • Insufficient level of awareness of the obligation imposed on the DNFBPs sector when it comes to dealing with PEPs **Recommendations 8 and 9** • The real estate agents, lawyers, notaries and other independent legal professionals and accountants have no knowledge of any CDD requirements whatsoever. **Recommendation 10** • The provisions of AML/CFT Act on record-keeping are generally not recognised, and the extent of data kept by the obliged institutions from this sector is dictated rather by the legal provisions applying directly their ore activities, than by the provisions of the AML/CFT Act on this. **Recommendation 11** • The knowledge of obligations of unusual transactions reporting and sector specific indicators is not sufficient enough.

4.2 Suspicious transaction reporting (R. 16)

(Applying R.13 to 15 and 21)

4.2.1 Description and analysis

Recommendation 16 (rated NC in the 3rd round MER)

675. Recommendation 16 was rated "*Non-Compliant*" in the 3rd round MER. The presence of hardly any reports from the DNFBP sector and the shortcomings regarding the reporting of TF were the main deficiencies underlying this rating.

676. DNFBPs are included in the list of reporting entities according to paragraph 1 (letter d to n of Section 5 of the AML/CFT Act. Namely, following entities are considered as DNFBPs in this regard:

"d) gambling game operator,
e) a postal undertaking,
f) a court distrainer,
g) an administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings under a special regulation,
h) an auditor, an accountant, a tax advisor,
i) a legal entity or a natural person authorised to mediate sale, rent or purchase of real estate,
j) an advocate or notary if he provides the customer with legal services related to
1. purchase or sale of real estate or ownership interests in a company,
2. management or safekeeping of funds, securities or other property,
3. opening or management of an account with a bank or a foreign bank branch or of a securities account or
4. establishment, operation or management of a company, an association of natural persons or legal entities, a special-purpose corporation or another legal entity,
k) a service provider of property management or a company service provider, unless it is an obliged entity under letters h) or j),
l) a legal entity or a natural person authorised to provide the services of organisational and economic advisor, the services of public carriers and messengers or forwarding services,
m) a legal entity or a natural person authorised to operate an auction hall, a legal entity or a natural person authorised to trade in works of art, collector's items, antiques, cultural monuments, items of cultural heritage, precious metals or gemstones, a legal entity or natural person authorised to place products made of precious metals or gemstones on the market or a legal entity or a natural person authorised to operate a pawnshop,
n) other person if so laid down by a special regulation."

Applying Recommendations 13-15

Requirement to Make STRs on ML/FT to FIU (c. 16.1; applying c. 13.1 & c.13.2 and SR. IV to DNFBPs)

677. The UTR reporting regime has already been described under Section 3.5 above. The weaknesses that applied to the financial sector also apply to DNFBPs. The AML/CFT Act provides for a general obligation to make a UTR on ML/TF directly to the FIU, and this obligation applies also to all DNFBPs without any exemptions.

678. All mentioned entities, except lawyers and notaries, are required to report unusual transactions under the same conditions of any other reporting entity from the financial sector. Dealers in precious metals and stones are required to report unusual transactions irrespective of the amount and nature of transactions, not just when they engage in cash transactions equal or above USD/€15,000.

Legal Privilege

679. Lawyers and notaries are required to report unusual transactions when they are engaged in activities listed in criterion 16.1 of the Methodology.

680. Lawyers are exempted from the obligation to report unusual transactions as well as to provide additional information and documentation based on a request from the FIU in circumstances when the information about the customer is obtained from the customer or in any other way during or in connection with:

a) processing legal analysis,
b) defending the customer in criminal law proceedings,
c) representing the customer in court proceedings or
d) providing legal advice related to the criminal or other court proceedings including legal consulting on the commencement or prevention of such a proceeding regardless of whether such information was received or obtained prior to, during or after such proceedings. (Section 22 of the AML/CFT Act)

681. Notaries, auditors, accountants and tax advisors are also exempted from the obligation to report unusual transactions as well as to provide additional information and documentation based on a request from the FIU in circumstances when the information about the customer is obtained from the customer or in any other way during or in connection with the provision of legal advice related to the criminal or other court proceeding including legal consulting on the commencement or prevention of such a proceeding regardless of whether such information was received or obtained prior to, during or after such proceedings. (Section 23 of the AML/CFT Act)

No Reporting Threshold for STRs (c. 16.1; applying c. 13.3 to DNFBPs)

682. The reporting obligation is suspicion based and applied irrespective of any threshold. This obligation is applicable for all obliged entities including DNFBPs.

Making of ML/FT STRs Regardless of Possible Involvement of Tax Matters (c. 16.1; applying c. 13.4 to DNFBPs)

683. All DNFBPs are required to report unusual transaction irrespective of possible involvement of tax matters.

Reporting through Self-Regulatory Organisations (c.16.2)

684. The AML/CFT Act does not allow lawyers, notaries, other independent legal professionals or accountants to send their UTRs to their appropriate self-regulatory organisations, but requires them to report directly to the FIU.

Legal Protection and No Tipping-Off (c. 16.3; applying c. 14.1 to DNFBPs) Prohibition against Tipping-Off (c. 16.3; applying c. 14.2 to DNFBPs)

685. The provisions of AML/CFT Act, as binding to all DNFBPs, protect the employees of DNFBPs from civil and criminal liability for breach of any restriction on disclosure of information if they report an STR to the FIU. Tipping-off by the employees of the DNFBPs is also prohibited.

Establish and Maintain Internal Controls to Prevent ML/FT (c. 16.3; applying c. 15.1, 15.1.1 & 15.1.2 to DNFBPs)

686. Paragraph 2 of Section 20 of the AML/CFT Act requires DNFBPs to have an internal program which stipulates a procedure applied while evaluating whether the transaction being prepared or carried out is unusual, a procedure applied from the moment of detecting an unusual transaction to its immediate reporting to the FIU including procedure and responsibility of employees evaluating the unusual transactions. This is, however, not sufficient for establishing that the obligation under R.16 have been fulfilled, as the internal controls are not explicitly ordered to be created.

Independent Audit of Internal Controls to Prevent ML/FT (c. 16.3; applying c. 15.2 to DNFBPs)

687. There is no obligation whatsoever for the DNFBPs to have and independent audit function.

Ongoing Employee Training on AML/CFT Matters (c. 16.3; applying c. 15.3 to DNFBPs)

688. Training requirements as set out in the AML/CFT Act stay valid and binding for all of the DNFBPs. As the evaluation team was advised during the on-site visit by the representatives of the DNFBPs sector, the obligation to provide training is fulfilled regularly. As it was mentioned, however, the poor recognition of the obligations imposed by the AML/CFT Act (especially those on CDD measures) hampers the overall effectiveness.

Employee Screening Procedures (c. 16.3; applying c. 15.4 to DNFBPs)

689. As described above, the Act on Gambling does have certain provisions related to employees and shareholder screening. However, there are no such provisions for other DNFBPs.

Additional Element—Independence of Compliance Officer (c. 16.3; applying c. 15.5 to DNFBPs)

690. The arguments and comments made above on the independence of the compliance officer are also applicable for DNFBPs. This means that there is no explicit obligation for the DNFBPs to appoint a compliance officer at the managerial level.

Applying Recommendation 21

Special Attention to Persons from Countries Not Sufficiently Applying FATF Recommendations (c. 16.3; applying c. 21.1 & 21.1.1 to DNFBPs)

691. As mentioned the external auditors are the only group which seems to be fully versed on responsibilities arising from the provisions of AML/CFT Act. This is no different when talking about the obligation to pay special attention to persons from countries not sufficiently applying FATF Recommendations. To the evaluation team's knowledge this standard is not recognised by most of the institutions form this sector.

Examinations of Transactions with no Apparent Economic or Visible Lawful Purpose from Countries Not Sufficiently Applying FATF Recommendations (c. 16.3; applying c. 21.2 to DNFBPs)

692. Although the legal framework as discussed previously also applies to the DNFBP, the awareness of the obligation is quite poor and not sufficient enough.

Ability to Apply Counter Measures with Regard to Countries Not Sufficiently Applying FATF Recommendations (c. 16.3; applying c. 21.3 to DNFBPs)

693. The shortcomings of the legal framework indicated in Section 3.5 of this report influence the implementation of this particular standard across the sector.

Additional Elements – Reporting Requirement Extended to Auditors (c. 16.5)

694. Both the auditors and accountants are obliged entities, and they must apply all rules set out in the AML/CFT Act. The only limitation to this is set out in Section 23 of the Act. According to this

section, an auditor or an accountant who performs its activities as an entrepreneur or a tax advisor does not have to report an STR or provide information to the FIU if it concerns the information about the customer obtained from the customer, or in any other way during or in connection with the provision of legal advice related to the proceedings referred to in Section 22, subsection 1, letter b) and c) including legal consulting on the commencement or prevention of the proceedings referred to in Section 22, subsection 1, letter b) and c), regardless of whether such information was received or obtained prior to, during or after such proceedings. This however cannot be seen as a deficiency in the light of criterion 16.4.

Additional Elements – Reporting of All Criminal Acts (c. 16.6)

695. There are no impediments in the legal system, which could allow DNFBPs not to report to the FIU when they suspect or have reasonable grounds to suspect that funds are the proceeds of all criminal acts that would constitute a predicate offence for money laundering domestically.

Effectiveness and efficiency

Applying Recommendation 13

696. Concerns over the ineffective implementation of requirements of R.16 by, especially the very low level of reporting from DNFBP is one of the main deficiencies identified in the 3rd round MER.

697. Leaving aside the refinements of requirements of relevant recommendations referred to in R.16 in the AML/CFT Act, given the statistics made available, the same concerns identified in the 3rd round MER over the effectiveness of the implementation in all aspects of the Recommendation remain valid. For instance, only 1 UTR has been received from lawyers (in 2006) and 8 from notaries since the adoption of 3rd round MER. Only 2 UTRs have been reported by real estate agencies a very low number of STRs has been reported by accountants and auditors. No data has been made available as to whether dealers in precious metals and stones have ever reported any UTRs. (For further details see table above) Before the adoption of the new AML/CFT Act, the largest number of unusual transaction reports was coming from car dealers, which are exempted from the list of obliged entities in the new Act. All other DNFBPs have submitted insufficient number of reports.

698. Although some outreach activities have been performed by the FIU, there is still a lot to be done in respect of the level of awareness of DNFBPs regarding reporting obligation. No guidelines have been issued to these sectors, except some indicators that are presented in the AML/CFT Act.

Applying Recommendation 14

699. It is apparent that all provisions of the AML/CFT Act which apply to financial institutions are also fully applicable to the DNFBP sector.

Applying Recommendation 15

700. There is no obligation for the compliance officer to be appointed at the managerial level, nor is there an obligation to maintain independent audit function.

701. The above fact has to be taken into consideration along with the poor outreach to this sector by the FIU. There are no sector specific guidelines whatsoever on AML/CFT issues and the effectiveness of the trainings is not satisfactory. This is due to a very low level of awareness of certain specific obligations applicable to those institutions (especially the obligation on CDD measures)

702. As the evaluation team was advised the number of on-site inspection cannot be deemed sufficient enough to reach effectively this sector. All this constitutes a serious deficiency.

Applying Recommendation 21

703. The shortcomings of the legislation pinpointed in Section 3.5 of this report hamper the overall application of R.16

4.2.2 Recommendations and comments

Applying Recommendation 13

704. Authorities should tailor and implement more comprehensive outreach and training programme targeted to DNFBPs to enhance the awareness and knowledge of UTR detection and reporting.

705. Guidelines and indicators for recognising suspicious transactions similar to those given to the banking sector in the Methodological guidance should also be issued for DNFBPs.

Applying Recommendation 15

706. The Slovak authorities should consider the way to meet the R.15 standards to DNFBPs in the field of appointing the compliance officer and maintaining independent audit function.

707. The poor outreach to this sector, unsatisfactory effectiveness of the trainings and an insufficient number of on-site inspections should be addressed by the Slovak authorities, preferably in a manner of an ongoing process.

708. There should be provisions related to employees and shareholders screening, which at this point only apply to gambling operators and other institutions that fall under the jurisdiction of the Gambling Act.

Applying Recommendation 21

709. When the legal framework is improved by the Slovak authorities it should also be applicable to the DNFBPs. The awareness raising programs should be also considered.

4.2.3 Compliance with Recommendation 16

	Rating	Summary of factors relevant to s.4.2 underlying overall rating
R.16	**PC**	• The same formal shortcomings under R.13, 15 and 21 equally apply to DNFBPs. **Applying Recommendation 13** • Serious lack of proper understanding of the reporting requirements among DNFBPs. • No indicators or guidelines provided to DNFBPs. • Serious concerns about the effectiveness of implementation in all aspects of Recommendation 16. • The same shortcomings as identified under R. 13 – 15, 21 and SR IV in respect of financial institutions apply to DNFBPs. **Applying Recommendation 15**

		• The Act on Gambling does have certain provisions related to employees and shareholder screening. However, there are no such provisions for other DNFBPs. • The poor recognition of the obligation imposed by the AML/CFT Act (especially those on CDD measures) hampers the overall effectiveness of the execution of training obligation. • Lack of an obligation for DNFBPs to appoint compliance officer at the managerial level and to maintain independent audit function. • Lack of an explicit obligation for DNFBPs to have internal controls or to appoint a compliance officer at the managerial level. • No independent audit function is required. • The trainings provided to this sector are not effective as the recognition of the obligations under the AML/CFT Act remains poor. **Applying Recommendation 21** • As the obligations arising from R.21 are not met in regard to financial institutions in general, they also do not apply to DNFBP.

4.3 Regulation, supervision and monitoring (R. 24-25)

4.3.1 Description and analysis

Recommendation 24 (rated PC in the 3rd ***round MER)***

Regulation and Supervision of Casinos (c. 24.1, c.24.1.1, 24.1.2 & 24.1.3)

710. The Act on Gambling games prescribes the supervision of casinos. According to Article 2 letter (a) of this act *"the operator of a gambling game is understood as a legal person that was granted an individual license (…) by a relevant body of the public administration or municipality, or a legal person that fulfilled the conditions of a general license issued by the Ministry of Finance of the Slovak Republic (…) and handed in a notification according to Section 19". Article 9 provides for a supervision of internet casions."*

711. The Public administration bodies in the field of gambling games are the MoF, the Tax Directorate of the Slovak Republic, and the Tax Offices.

712. The MoF is authorised to exercise controls according to a special regulation over observance of the Act on Gambling games and other generally binding legal regulations by its own means or the means of the Tax Directorate of the Slovak Republic, Tax Offices and Municipalities of the Slovak Republic. The MoF is also charged with co-ordination of the Tax Directorate of the Slovak Republic methodically, tax offices and municipalities in the field of supervision exercised. It is also authorised to grant license for all gambling games operators, but it has an exclusive power to grant license for casinos.

713. At the time of the on-site visit there were three people in the MoF designated for on-site visits and four designated for the licensing of gambling operators. As indicated by the MoF there were

302 inspections in eight gambling places in the year 2009. As the evaluation team was advised there is no co-ordination of inspection plans between the FIU and the MoF, and the MoF does not provide the gambling operators with any training on the AML/CFT issues.

714. It is also of concern to the evaluators that the level of thoroughness of on-site visits related to AML/CFT issues in gambling operators may not be very high.

715. The Tax Directorate is entitled to create, maintain and operate a tax information system in the field of the operation of gambling games, keeping a central register of the operators of gambling games, and methodically co-ordinating the tax offices during the operation of the tax information system in the field of gambling games.

716. The Tax Office and the Municipalities are entitled to exercises supervision over observance of the Gambling Act, other generally binding legal regulations and conditions determined in the license. The difference between those two bodies is that the Tax Office may do so in respect of the license granted or issued by the Ministry and that it is also a second degree body of appeal for municipalities in this matters. The Municipality may only exercise control over bodies to which they have granted a license.

717. During the process of granting the license the proper authority is obliged to receive a full information on all person engaged with the gambling operator (in respect of them holding any shares or taking part in the profits from this establishment), as stated in paragraph 4 of Article 20 of the Gambling Act. The said act also defines the term "respectable person", as someone, who has not been finally convicted of an economic criminal offence, criminal offence against order in public matters or criminal offence against property, or other intentional criminal offence.

718. The integrity and respectability of persons engaged in the activities of a gambling operator must be maintained through the entire operation (also after granting a license), as stipulated in Article 35 of the Act.

719. According to Article 54 of the Gambling Act, if the authority, which has the power to conduct on-sites, establishes that supervised entity has violated the provisions of the said Act, specific acts or other legal regulations may impose the following sanctions:

"a) measures for removal or remedy of the established discrepancies, including the period for their fulfilment and the duty to inform the supervisory body on their fulfilment within the determined period,
b) submission of special statements, reports and notices,
c) termination of non-permitted activity,
d) suspension of operation of a gambling game,
e) fine,
f) sanction interest in the amount and in the cases according to Section 2,
g) suggestion to the ministry or municipality for withdrawal of the individual license."

720. The evaluators believe that the supervision system over gambling operators is properly co-ordinated, and that the AML/CFT issues are being taken into account during supervisions conducted. The competent authorities have been designated, and they also have adequate powers, as stated above, to ensure that the persons engaged in the activities of the gambling operators are of good integrity and are respectable.

Monitoring and Enforcement Systems for Other DNFBPs-s (c. 24.2 & 24.2.1)

721. Section 5 of the AML/CFT Act provides for a catalogue of entities, who are obliged to follow the provisions of this Act. Setting aside the financial institutions, and other institutions already mentioned in this report, the catalogue comprises:

- a postal undertaking,
- a court distrainer,
- an administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings under a special regulation,
- an auditor, an accountant, a tax advisor,
- a legal entity or a natural person authorised to mediate sale, rent or purchase of real estate,
- an advocate or notary (under certain conditions),
- a service provider of property management or a company service provider, unless it is an obliged under other provision of the said act
- a legal entity or a natural person authorised to provide the services of organisational and economic advisor, the services of public carriers and messengers or forwarding services,
- a legal entity or a natural person authorised to operate an auction hall, a legal entity or a natural person authorised to trade in works of art, collector's items, antiques, cultural monuments, items of cultural heritage, precious metals or gemstones, a legal entity or a natural person authorised to place products made of precious metals or gemstones on the market or a legal entity or a natural person authorised to operate a pawnshop,
- other person if so laid down by a special regulation.

722. All of these institutions are under the supervision of the FIU. Some of them, like the lawyers, auditors, accountants, tax advisors have their own SROs, which does not limit the powers of the FIU for AML/CFT related supervision.

723. It is apparent from the level of awareness of the DNFBP that more actions should be taken to remedy this situation, or to take enforcement measures. As the evaluation team was advised by the FIU, around 40% of all on-site visits conducted in 2009 and 2010 were aimed at this sector. It is, however, unclear if there is a strategy for the FIU to address the issue of supervision over DNFBPs.

724. The current level of on-site inspections and outreach to this sector may only be deemed as theoretical.

725. It is also highly unlikely that the supervision over this sector can be conducted effectively by the FIU, given the size of this unit, and the number of entities to be supervised. The statistics on on-site visits also support this argument.

Recommendation 25 (rated NC in the 3rd round MER)

Guidance for DNFBPs other than feedback on STRs (c. 25.1)

726. Section 26 of the AML/CFT Act provides a legal basis for provision of feedback to all the reporting entities including DNFBPs. The evaluation team was advised, the FIU wrote to all the associations, chambers and professions of the reporting entities to notify them about it's website. The FIU has requested these organisations and profession associations to provide e-mail contacts. The goal of this was for the organisations and profession associations to inform their members. During the interviews on-site, the evaluation team was also assured that there is a functioning oral feedback mechanism in place between the FIU and DNFBPs.

727. Criterion 25.1 requires the authorities to issue guidelines to the DNFBP sector. The evaluation team notes that the FIU has provided guidelines to gambling operators, entrepreneurs dealing with cash exceeding the value of €15,000, auditors, accounts, executors, real-estate agents and advocates.,

Feedback (applying c. 25.2)

728. As mentioned previously in the rare cases of UTR reporting by the DNFBP sector, the feedback, aside from guidelines, is provided by the FIU.

729. More focus should be placed on improving the co-operation with the DNFBP sector in the respect of feedback on STRs. The financial institutions are generally satisfied with the feedback they receive, but it is worth analysing whether the feedback should be more detailed and prompt, as it was one of the major concerns of the financial sector. The evaluators also strongly believe that prompt and detailed feedback can largely improve the effectiveness of implementing Recommendation 25.

Adequacy of resources supervisory authorities for DNFBPs (R. 30)

730. The resources of the FIU are still not sufficient enough to deal with the scope of supervision prescribed by the AML/CFT Act. The FIU employs 37 police officers and one civil servant, and the part responsible for controls employs six people (plus one person designated as a head of this office). As mentioned before the MoF supervising gambling sector is also understaffed.

Effectiveness and efficiency (R. 24-25)

731. The deficiencies described above have a direct impact on the issue of effectiveness. It is utterly impossible to conduct a full scope of supervision over the DNFBPs without an increase in staff of the FIU.

732. The lack of awareness in this sector may and should be attributed to a number of factors. Sector specific guidelines for the sectors other than those already addressed by the FIU should also be issued.

4.3.2 Recommendations and comments

Recommendation 24

733. It is apparent that the FIU needs more resources to fully embrace the supervision requirements over the DNFBP sector, as the resources now present can only be deemed sufficient as far as the supervision over the financial sector goes.

Recommendation 25 (c.25.1 [DNFBPs])

734. There is an urgent need for sector specific guidelines on AML/CFT issues to the DNFBPs other than already covered by the FIU.

735. More detailed and prompt case-by-case feedback should be provided for the DNFBP sector.

4.3.3 Compliance with Recommendations 24 and 25 (Criteria 25.1, DNFBPs)

	Rating	Summary of factors relevant to s.4.3 underlying overall rating
R.24	**PC**	• No clear strategy for DNFBP supervision demonstrated to the evaluators. • Not sufficient outreach to this sector, also in the way of on-site inspections. • Effectiveness concerns about the supervision of DNFBPs by the FIU.
R.25	**PC**	• Sector specific guidelines for DNFBPs do not cover the entire sectors. • More detailed and prompt case-by-case feedback should be provided.

4.4 Other non-financial businesses and professions/Modern secure transaction techniques (R.20)

4.4.1 Description and analysis

Recommendation 20 (rated PC in the 3rd round MER)

736. In Section 5 of the AML/CFT Act obliged entities include the following additional DNFBPs:
- service providers of property management or company service providers,
- legal entities or natural persons authorised to provide services of organisational and economic advisor,
- the services of public carriers and messengers or forwarding services,
- auction hall operators,
- legal entities or natural persons authorised to trade in works of art, collector's items, antiques, cultural monuments, items of cultural heritage and pawnshop operators,
- a postal undertaking,
- a court distrainer,
- an administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings under a special regulation.

Notwithstanding current levels of compliance of the Slovak system generally with the FATF Recommendations 5, 6, 8-11, 13-15, 17 and 21 (discussed above), these Recommendations apply to these additional businesses and professions in as much as they apply to other obliged entities.

737. Financial market participants consist mainly of banks, foreign bank branches, other payments services providers and e-money institutions. Currently, more then 30% of all cashless transactions in the Slovak Republic are made by cards. At the end of 2009 there were 5,080,145 active debit and credit cards, of which 79% were debit cards and 21% credit cards. Although ATM cash withdrawals still dominate, the trend shows a dynamic growth in card payments, especially since the Euro is the national currency.

738. As the evaluation team was informed, the Slovak Republic is ready for SEPA, (The Single Euro Payments Area), which is a policy-maker-driven EU integration initiative in the area of payments designed to achieve the completion of the EU internal market and monetary union.

739. It is, however, still roughly unclear whether any further measures were taken to encourage the development and use of modern and secure techniques for financial transactions that are less vulnerable to ML.

4.4.2 Recommendations and comments

740. The Slovak authorities are encouraged to develop measures to encourage the development and use of modern and secure techniques for financial transactions that are less vulnerable to ML.

4.4.3 Compliance with Recommendation 20

	Rating	Summary of factors underlying rating
R.20	**LC**	• No national overreaching strategy on the development and use of modern secure techniques.

5 LEGAL PERSONS AND ARRANGEMENTS AND NON-PROFIT ORGANISATIONS

5.1 Legal persons – Access to beneficial ownership and control information (R.33)

Recommendation 33 (rated PC in the 3rd round MER)

5.1.1 Description and analysis

741. Recommendation 33 was rated *"Partial Compliant"* in the 3rd round MER on the ground that Slovak Law did not require adequate transparency concerning beneficial ownership and control of legal persons, although it required some transparency with respect to immediate ownership. The report also noted that access to information on beneficial ownership and control of legal person, when there was such access, was not always timely. Therefore, Slovakia was recommended to review its commercial, corporate and other laws with a view to taking measures to provide adequate transparency with respect to beneficial ownership.

Legal framework

742. The Slovak Civil Code (the Act No 40/1964 Coll.) describes the types of legal persons and legal entities that can be established or created, or which can own property. Registration of legal persons (commercial companies) is regulated by the Act no. 513/1991 Coll. Commercial Code as amended and the Act no. 530/2003 Coll. on Commercial Register and Collection of Deeds. Registration of other legal persons is regulated by particular laws such as the Act No. 34/2002 Coll. on Foundations and the Act No. 83/1990 Coll. on Association of Citizens as amended. The Section 27 of the Commercial Code contains basic provisions on commercial register, collection of deeds and their content. The Act No. 530/2003 Coll. on Companies Register contains more detailed provisions of the companies register and the collection of deeds. No amendments have been made to this legislation since the adoption 3rd round MER with regard with a view to implement the requirements of Recommendation 33. Therefore, the legal description of the system of registration of legal persons particularly companies in the 3rd round MER (See Sections 1.4 and 5 of the MER) remains apt.

Measures to prevent unlawful use of legal persons (c. 33.1)

743. As noted in the 3rd round MER, the documents which need to be submitted to the Commercial Registry are the constitutive documents (the collection of deeds i.e. the memorandum of association or deed of establishment), a deed proving trading or similar authorisation for performance of activities registered with the Commercial Registry as the company's scope of business, if such authorisation is required, and a statement of the administrator of contributions to the registered capital of business companies and co-operatives. The name and date of birth of persons authorised to act on behalf of registered persons (e.g. directors of limited liability companies), persons that are the members of supervisory boards of registered persons, registered individuals (e.g. partners in the case of partnerships), directors of enterprises of foreign persons or directors of organisational units (branches) of enterprises of foreign persons, promoters, liquidators, bankruptcy administrators and forced administrators and their deputies are the information that need to be registered with the Commercial Registry. Under Section 2 of Act no. 530/2003 Coll, any company listed in the Business Register must provide information, inter alia, on the company's name, ID number, line of business, legal form and registered capital, information on the company's statutory and supervisory

bodies or partners in the company, as well as information on any liquidation or similar proceedings which the company has undergone. However, no information was provided by the authorities on the registry requirements for associations and foundations.

744. Slovak law still does not provide for information about the beneficial ownership of companies in the way that "beneficial owner" is defined in the Glossary to the FATF Methodology (i.e. who ultimately owns or has effective control). This is particularly the case where one company buys shares in another company. In the meeting with the representatives of the Company's Registrar, the evaluators were informed that if one of the shareholders is a company, the Company Registrar would not request a registration certificate. As a result, the Company Registrar would not be aware of whether such a company actually exists. In addition, the examiners were told that it was not the function of the Commercial Registry to verify the accuracy of the information provided. In a nutshell, there is no legal obligation in the Slovak legislation to register beneficial ownership information and there is no any other measure exists that ensures adequate transparency concerning the beneficial ownership information.

745. The lack of transparency is even greater regarding sale of shares, for which the only documents required are a contract of sale and a decision of the General Assembly approving the transfer.

746. The Slovak law, although requiring some transparency with respect to immediate ownership, does not require adequate transparency concerning the beneficial ownership and control of legal persons.

Timely access to adequate, accurate and current information on beneficial owners of legal persons (c. 33.2)

747. Full details of what is deposited at the Registry may be inspected by the competent authorities or the public. Every person has the right to inspect these documents and make copies of them after paying the Court's fees. In addition, *per* Article 12(7) of 530/2003 Coll. Act of 28 October 2003, public administration bodies may inspect documents serving the basis for registration even without paying the fees. In addition, information in the Commercial Registry is available on-line. Information can be found on-line relating to, *inter alia*, natural persons, and statutory representatives, and proxies, members of supervisory boards, partners and founders. However, share holder information is not generally available on-line. Art. 5(5) of the same Act requires natural persons inscribed in the Registry and natural persons authorised to act in their name to file an application for change of information within 30 days from when the information ceases to be accurate. Under Article 11(1) (a), a fine of up to €3,310 can be imposed for a failure to meet this obligation. The Slovak authorities provided detailed information about penalties for failure to update information issued by the Register Court. According to this information, fines or other sanctions have been imposed in over 2,300 cases since 2005. Regarding beneficial ownership, the NBS has access to beneficial ownership information by virtue of Article 3, para. 1-2 of the FMS Act. However, no information was provided to the evaluators regarding the timely access of other competent authorities to this information, including law enforcement and the FIU.

Prevention of misuse of bearer shares (c. 33.3)

748. According to the Slovak Authorities, bearer shares are allowed by the Securities Act; however, such shares can only have de-materialised book-entry form. Respective provisions determining these facts are Articles 10 and 11 of the Securities Act. Article 10(3) of the Securities Act sets out that bearer shares, shares in closed-end investment funds, bearer shares in open-end investment funds, bonds, investment certificates, and treasury bills must have the form of book entry securities.

749. Furthermore, all book-entries are registered in the Central Securities Depository (CSD) on client's accounts or in registers of CSD members and all accounts must include identification data of the account owner. Articles 109 and 110 contain the details of the access to such information by the competent authorities (including the FIU and the NBS). According to Slovak authorities, law enforcement, regulatory, supervisory and other competent authorities must rely on their investigative and other powers to obtain access to information on beneficial owner information. Although obliged entities must establish beneficial ownership pursuant to paragraph 1 of Section 10 of the AML/CFT Act, there are no special measures in place with regard to transparency of beneficial ownership in companies with bearer shares.

Additional element - Access to information on beneficial owners of legal persons by financial institutions (c. 33.4)

750. The evaluation team was advised only about the on-line access to the court register data, which do not cover beneficial ownership in all cases. It is then on the financial institutions to employ measure adequate to make themselves aware of the identity of the beneficial owner. Bearing in mind the level of awareness in the financial sector, the evaluation team is convinced that such measures are being taken by the financial institutions in order to comply with the Slovak legislation.

5.1.2 Recommendations and comments

751. Given the explanations received, no comprehensive review appears to have been made on commercial, corporate, and other laws with the view to taking measures to provide adequate transparency with respect to the beneficial ownership as recommended in the 3rd round mutual evaluation report. Therefore, the deficiencies regarding this Recommendation still appear to remain valid. The evaluators of this round reiterate the finding of the 3rd round evaluators that Slovak law still does not require adequate transparency concerning beneficial ownership and control of legal persons.

752. Slovakia is recommended to review its commercial, corporate and other laws with a view to provide transparency with respect to beneficial ownership.

5.1.3 Compliance with Recommendations 33

	Rating	Summary of factors underlying rating
R.33	**PC**	• Lack of adequate transparency concerning beneficial ownership and control of legal persons. • Access to information on beneficial ownership and control of legal persons, when there is such access, is not always timely. • No measures to ensure the adequacy, accuracy and currency of the beneficial ownership information. • Transparency of bearer shares.

5.2 Non-profit organisations (SR.VIII)

5.2.1 Description and analysis

Special Recommendation VIII (rated NC in the 3rd round MER)

753. Special Recommendation VIII was rated *"Non-Compliant"* in the 3rd round MER on the ground that no special review had been undertaken of the risks in the NPO sector. The existing financial transparency and reporting structures that were available for foundations did not amount to effective implementation of c.VIII.2 and VIII.3. Therefore, Slovakia was recommended to consider to ways in which effective and proportionate oversight of the NPO sector can be achieved in the context of SR VIII.

Legal framework

754. As noted in the 3rd round MER, the NPO sector comprises primarily foundations and associations. As of 31 December, 2010, there were 409 foundations, 559 non-investment funds, and 1409 non-profit organisations registered in the Slovak Republic. Whilst foundations are regulated by the Act No. 34/2002 Coll. on Foundations and on amendments to the Civil Code, associations are regulated by the Act No 83/199-0 Coll. No amendment has been reported in the legislative framework of the NPO sector since the adoption of the 3rd round MER. Therefore, the description of their registration processes, obligation to submit an annual report and the information registered that were set out in the 3rd round MER remain valid.

755. Slovak authorities do not think that there is a risk of NPOs being abused for TF purposes or terrorist attacks in the Slovak territories.

Review of adequacy of laws and regulations (c.VIII.1)

756. Though authorities argue in the MEQ that the risk analysis regarding NPOs and their abusing, especially with regard to TF, was under consideration while preparing the new AML/CFT Law, the evaluation team did not receive any substantial information which demonstrates that, since the adoption of the 3rd round MER, Slovakia has reviewed the adequacy of its legislation that relates to the NPO sector as a whole and has conducted any periodic reassessment by reviewing new information on the sector's potential vulnerabilities to terrorist activities.

Outreach to the NPO Sector to protect it from Terrorist Financing Abuse (c.VIII.2)

757. No outreach has been undertaken to the NPO sector with a view to protecting the sector from terrorist financing abuse as required by c.III.2. The evaluators were informed that there has been no special guidance on the risk inherent in the sector of NPOs.

Supervision or monitoring of NPO-s that account for significant share of the sector's resources or international activities (c.VIII.3)

758. The evaluators were informed that while foundations are legally obliged to submit a list of donors, associations are not required to present a list of donors. The report is read by the registration body and checked whether the foundation functioned in accordance with its statute.

759. The requirement of foundations to submit an annual report to the registration body might provide a level of transparency, and NPOs receiving funds from the government or from the EU are supervised by the Financial Control Administration incorporated under the Ministry of Finance in

connection with disposal of such funds. However, these mechanisms are far from being an effective supervision or monitoring mechanism for those NPOs which account for a significant portion of the financial resources under control of the sector and a substantial share of the sector's international activities. In fact, apart from providing the information about the numbers and types of NPOs, unfortunately no information was provided to the evaluators on those specific NPOs that control significant resources within the NPO sector or which have significant international activities. Therefore, the evaluators concluded that those part of the NPO sector with significant economic resources had not been specifically identified for effective supervision or monitoring.. It should also be noted, as pointed out in the 3rd round MER, the registration body is not a supervisory or monitoring body, but performing primarily registration function. In addition, the Central Registry is not aware of the risk of financing of terrorism with regard to NPOs and they do not check names in the registry against the list of designated persons.

Information maintained by NPO-s and availability to the public thereof (c.VIII.3.1) Licensing or Registration of NPO-s and availability of this information (c.VIII.3.3)

760. Both associations and foundations are registered in the Central Registry managed by the Ministry of Interior, which is public and available on the Internet (http://portal.inves.sk/registre). The data recorded in the Central Registry includes: name and residence, identification number, establishment data, purpose of establishment, name and residence of founders, and money and other assets deposited by founders. The central registry does not seem to include, however, the identity of persons) who own, control or direct their activities, including senior officers, board members and trustees. Nevertheless, the evaluators were informed that the registration body (the Section of Public Administration, Internal Affairs Department) with which the team met stated that they have no means to identify and verify the founder of the NPO, and even have no legal obligation to do so. In turn, the evaluators were advised that the FIU have referred to the Central Registry with four requests to receive information.

Measures in place to sanction violations of oversight rules by NPO-s (c.VIII.3.2)

761. The evaluators were told that if the registration body discovers any violation of law from the annual report, it can call the foundation to eliminate the violations and to take measures. In the case of non-compliance and repeated calls to eliminate the violations, the body then can send a motion to the court to dissolve the foundation. It is also authorised to apply fines for certain violations. The Registrar of Foundations is authorised to impose a fine for failure to submit annual report under Section 36 of Act No. 34/2002 on foundations. In case of any shortcomings, the registrar requests that the foundation correct them. If the foundation fails to do so, registrar must submit a request for cancellation of foundation to court. The Registrar of NPOs is authorised to submit a request to the court for cancelation of an NPO in case of any shortcomings not eliminated by the NPO

Maintenance of records by NPO-s, and availability to appropriate authorities (c.VIII.3.4)

762. No obligation appears to have existed in place for NPOs to maintain, for a period of at least five years, and make available to appropriate authorities, records of domestic and international transactions that are sufficiently detailed to verify that funds have been spent in a manner consistent with the purpose and objectives of the organisation.

Measures to ensure effective investigation and gathering of information (c.VIII.4)Domestic co-operation, co-ordination and information sharing on NPO-s (c.VIII.4.1); Access to information on administration and management of NPO-s during investigations (c.VIII.4.2); Sharing of information, preventative actions and investigative expertise and capability, with respect to NPO-s suspected of being exploited for terrorist financing purposes (c.VIII.4.3)

763. Apart from the annual reporting obligation for foundations, the investigative powers of the Slovak law enforcement authorities as set out in the SCPC and the Police Act are also applicable to the NPO sector. Related information is accessible for all investigation authorities.

764. No specific provisions apply to permit domestic co-operation and information sharing outside the usual criminal investigation framework. Full access to information on the administration and management of a particular NPO can be obtained during the course of an investigation, as soon as there is a legal basis for the information to be recorded. The legal framework allows for information sharing at investigation level as well as administrative level.

Responding to international requests regarding NPO-s – points of contacts and procedures (c.VIII.5)

765. Since NPOs are not obliged entities, the usual points of contact and procedures are not relevant. The Slovak authorities did not indicate any alternative points of contact relevant to these bodies.

Effectiveness and efficiency

766. Although, there is some transparency and reporting structures regarding some NPOs (e.g. Foundations), the system which has been put in place is insufficiently comprehensive in its present form. There remains a pressing need to address SR VIII. This should be accompanied by significant awareness raising activities for both the relevant government departments and the NPO sector.

5.2.2 Recommendations and comments

767. Slovak authorities should review the risks of terrorist financing in the NPO sector, as well as the current system of laws and regulation in this field so as to adequately address the risks that this sector presents.

768. The authorities should also improve the supervision over the NPOs to ensure that all types of NPOs are under appropriate supervision with regard to the risks of financing of terrorism.

769. Awareness raising measures need to be adopted relating to the NPO sector on the risk of terrorist abuse and available measures to protect the sector against such abuse.

5.2.3 Compliance with Special Recommendation VIII

	Rating	Summary of factors underlying rating
SR.VIII	**NC**	• No risk assessment of NPOs has been undertaken, although there is some transparency and annual reporting structure for foundations. • No review of the adequacy of legislation to prevent the abuse of NPOs for TF has been undertaken. • Authorities do not conduct outreach or provide guidance on TF to the NPO sector. • There is no supervision or monitoring of the NPO sector as envisaged by the Interpretative Note to SR VIII. • No obligation for keeping detailed domestic and international transaction records. • 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.

6 NATIONAL AND INTERNATIONAL CO-OPERATION

6.1 National co-operation and co-ordination (R. 31 and R. 32)

6.1.1 Description and analysis

Recommendation 31 (rated PC in the 3rd round MER)

Effective mechanisms in place for domestic co-operation and co-ordination in AML/CFT (c.31.1)

770. The FIU under the auspices of the Ministry of Interior established in 2008 a working group named Interagency Integrated Group of Experts (hereinafter referred to as IIGE). This group comprises the representatives of the FIU, the National Bank of Slovakia, the Ministry of Justice, the Ministry of Finance, the General Prosecutor's Office, the Slovak Intelligence Service and the Customs Directorate, and the Tax Directorate and in case of need the representatives of other bodies too. The evaluation team was advised that the IIGE meets regularly, at least 3 times a year. The Slovak authorities have provided the evaluators with the Decision of Interagency Expert Co-ordination Body for Fighting Criminality, No. 5/2008 from 27 October 2008, according to which the IIGE was established. However, the evaluators were not provided with minutes or other documents which have resulted from these meetings.

771. The IIGE in 2009 is reported to have worked with a working plan with identified areas, which should be addressed (e.g. creation of a central registry of bank accounts, possible introduction of cash transactions limitation by threshold, co-ordination of the AML/CFT Act's enforcement among bodies directly engaged in checking the compliance with the legal provisions, common interpretation and understanding and presentation of the preventive law provisions, etc.).

772. The interlocutors met on-site were aware of the existence and work of this group. Some confusion among authorities still exist on the mandate of this group and his correlation with some other groups mentioned like the Interagency Expert Co-ordination Authority for Combating Crime (MIKO) Group which appear to be the co-ordination group on a level of ministers while MISO or IIGE group is an expert group dealing with AML/CFT issues.

773. The FIU, as a lead authority of the Slovak AML/CFT regime, does not however seem strongly located enough to co-ordinate the work of such a group. Furthermore there was little knowledge (in the case of the MoF) on how to signal on any systematic problems in the country' AML/CFT regime, should such a need arise.

774. The said group therefore can be treated as a national body for strategic co-ordination between relevant authorities, but its role and the role of the FIU within this group could be strengthened. It is still an issue to be addressed that the FIU does not receive proper feedback from the law enforcement bodies on cases they disseminated. It is also worth mentioning in this context that more statistical feedback from all of the participants in this group may be a factor strengthening the national co-operation, which at present stage is low.

775. There seems to be a very good co-operation between the FIU and the National Bank of Slovakia especially in the area of outreach and providing guidance to entities from the financial sector. This co-operation was formalised in 2002 by signing an MOU which was amended later in

2004 and 2006. Cooperation between the FIU and law enforcement bodies is based on Act on Police Force and internal procedures within the Police, given that the FIU is a division in it.

776. The Slovak authorities rely on the general provision of the Law on State Administration which obliges all state bodies to co-operate and provide the widest possible assistance to other state bodies. Concrete models of day-to-day operational co-operation like task forces or designating liaison officers etc., are not widely used. Various state bodies concentrate on their specific areas of competence being rather isolated in their work. This point was raised also in the 3rd round MER and while some steps have been taken to improve the existing situation, there is still a lot to be done in this regard.

Additional element – Mechanisms for consultation between competent authorities and the financial sector and other sectors (including DNFBPs) (c. 31.2)

777. The FIU has established various mechanisms for consultation with the financial sectors and DNFBPs. All obliged entities met on-site were aware of the existence of the FIU website indicating that it is widely used by them. Various associations of obliged entities reported that they regularly receive guidance and useful information by e-mail form the FIU, which is later disseminated to all members. The evaluators also noted the existence of a very useful co-operation on a daily basis since all obliged entities reported that they are free to make a direct call to the FIU if there is any issue to be solved. The private sector representatives were generally satisfied with the quality and effect of such co-operation.

Review of the effectiveness of the AML/CFT system on a regular basis (Recommendation 32.1)

778. It seems that the IIGE does not have in its mandate the collection and reviewing of statistical or other information with regard to effectiveness of the system. There is no proof whatsoever of any collective review of the Slovak system done at any other level. The IIGE has been mandated to work on "unification and consolidation of process of collecting the statistical data related to ML and TF kept by the Ministry of Interior of the Slovak Republic, the General Prosecutor's Office and the Ministry of Justice of the Slovak Republic", but authorities have not provided the evaluators with any of the results in this regard. The most comprehensive statistics are maintained by the FIU. These statistics, although helpful, need improvement in their substance because the feedback given to the FIU does not contain sufficient data on ML or TF cases apart from the investigations of other criminal offences. In other words, while the FIU is obliged to disseminate cases on all criminal offences, which are done in majority of those cases (approximately 20% of all cases disseminated relates to ML), statistics received on investigations and prosecutions triggered by that dissemination do not contain the information on what criminal offence these actions are taken.

Recommendation 30 (Policy makers – Resources, professional standards and training)

779. Apart from general data received, the Slovak authorities have not provided any details on the allocation of other resources used to set up and maintain the AML/CFT system on the policy level. No information was made available on training of policy makers. Professional standard requirements are set out in the law and other relevant internal normative acts and codes on professional standards. Thus it was not demonstrated that requirements under Recommendation 30 for policy makers of competent authorities are met.

Effectiveness and efficiency

780. There is no proof whatsoever of any collective review of the Slovak system done at any level. Although some mechanisms exist, both legal and institutional, in place to co-ordinate activities the AML/CFT system, it seems that these mechanisms are not utilised sufficiently. While some

progress has been achieved in addressing the recommendations made in the 3rd round MER, there is still a lot to be done in this regard.

781. Co-operation on the national level still seems to be a façade rather than an instrument relevant in co-ordinating the entire AML/CFT regime.

6.1.2 Recommendations and Comments

Recommendation 31

782. Slovak authorities should consider taking steps to strengthen the IIGE perhaps on a more senior level. The issue of the weak position of the FIU, which is widely recognised as the leading authority in the AML/CFT system has already been noted earlier in this report.

783. More effective mechanisms are needed at operational level. Authorities should consider creating joint investigative teams or other forms of interagency co-ordination mechanisms, perhaps lead by prosecutors, in order to investigate and bring before the courts more money laundering cases which are related to major proceed-generating criminal offences.

784. Although some steps have been taken to improve national co-operation, all recommendations and comments under Recommendation 31 in the 3rd round MER remain valid.

Review of the effectiveness of the AML/CFT systems on a regular basis (Recommendation 32.1)

785. Slovak authorities should review the effectiveness of the system for AML/CFT on a regular basis.

786. The authorities should also:

- undertake an on-going analysis of the risks of ML/FT (vulnerabilities, sectors at risk, trends, etc) to streamline its AML/CFT strategy and efforts as necessary;
- pursue current efforts and develop the strategic and collective review of the performance of the AML/CFT system as a whole.

Recommendation 30 (Policy makers – Resources, professional standards and training)

787. The Slovak authorities should satisfy themselves that there are adequate resources allocated to set up and maintain the AML/CFT system on the policy level and that policy makers are appropriately skilled and provided with relevant training.

788. It seems necessary to provide additional resources to the FIU to allow more detailed co-ordination on the national level.

6.1.3 Compliance with Recommendations 31 and 32 (criterion 32.1 only)

	Rating	Summary of factors underlying rating
R.31	**PC**	• Lack of sufficient co-ordination between major players of the AML/CFT regime. • More effective mechanisms needed to co-ordinate at the operational level. • More detailed statistics are required across the board to assist proper

		co-ordinated policy analysis. • The mechanisms in place not utilised effectively.

6.2 The Conventions and United Nations Special Resolutions (R. 35 and SR.I)

6.2.1 Description and analysis

Recommendation 35 (rated LC in the 3rd round MER) & Special Recommendation I (rated PC in the 3rd round MER)

Ratification of AML Related UN Conventions (c. R.35.1 and of CFT Related UN Conventions (c. SR I.1)

789. As set out in the 3rd round MER, Slovakia is party to the Vienna and Palermo Conventions, as well as to the 1999 United Nations International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention).

790. The Slovak authorities submitted a table with comparison of the relevant provisions of the Vienna Convention and Palermo Conventions. According to the table the relevant articles of the Vienna & Palermo Conventions are covered, *inter alia*, by the Criminal Code, Act no. 460/1992 Coll - the Constitution of the Slovak Republic, Act no. 171/1993 2 Coll – on Police Forces etc.

Implementation of Vienna Convention (Articles 3-11, 15, 17 & 19, c. 35.1) Implementation of Palermo Convention (Articles 5-7, 10-16, 18-20, 24-27, 29-31 & 34, c.35.1)

791. The Slovak Authorities state that Articles 231, 232, 233 and 234 cover the provisions of Article 3(1)(b) of the Vienna Convention, Articles 129, 141 and 296 cover the provisions of Article 3(1)(c) of the Vienna Convention, and all the abovementioned articles cover the provisions of Article 6 of the Palermo Convention.

792. As stated above, Sections 231 and 233 criminalise money laundering offences largely in line with the elements listed in the Vienna and Palermo Conventions. However, as noted in sections 2.1 and 2.2 above, the following uncertainties and shortcomings appear to exist:

- Under the Conventions, acts of laundering should be criminalised when committed with knowledge that the property was derived from an offence, even when there is no intent to conceal (with the exception of the acts listed in Article 3(1) (b) (i) of the Vienna Convention and Article 6 (1) (a) of the Palermo Convention). Section 233 of the SCC requires the existence of a purposive element in order for an act to constitute an ML offence (specifically, intent to conceal or disguise the illicit origin of the property or frustrate its seizure, forfeiture or confiscation). Actions committed without any such intent, but only with knowledge that the property was derived from an offence are generally covered under Section 231. However, there are certain cases in which the scope of Section 231 is overly limited, which means that certain acts are not criminalised unless they are committed with intent to conceal, and thus fall under Section 233. Specifically, Section 231, by its nature, does not cover actions committed by the offender himself. Therefore, any acts committed by the offender himself with knowledge of the criminal source but without intent to conceal would not be covered by Section 231 or Section 233, and are therefore not criminalised. This deficiency severely limits the scope of the self-laundering prohibition and does not meet the requirements of the Convention. Similarly, Section 231 only covers acts of concealing, transferring, leasing or accepting a thing as a deposit. Therefore, other acts, including acts of possession or use, are not covered by any provision of the SCC when committed with knowledge of the criminal source of the property. This does not meet the requirements of the Conventions, which require that "the acquisition,

possession or use of property, knowing, at the time of receipt that such property was derived from an offence..." be criminalised (Article 3(1) (c) (i) of the Vienna Convention).

- As stated above, the Slovak authorities referred to sections 45-50 of the CCP regarding protection for the rights of bona fide third parties. However, only section 45 of the CCP is relevant to this issue. Section 45 provides that any party whose thing was seized has the right to participate in the legal seizure proceedings. Moreover, the protection provided is only procedural, rather a guarantee of substantive rights (with the exception of pledges and mortgages, which are provided with substantive protection). This provision does not comply with article 5(8) of the Vienna Convention and article 12(8) of the Palermo Convention.

793. The trafficking in narcotics and other drug related offences are criminalised by virtue of the SCC (Sections 171-174). The SCC provides for the confiscation of proceeds derived from drug related offences and narcotics and instrumentalities in drug related cases and associated ML. Legislation also provides extradition for all offences and MLA is available. Controlled delivery is available as an investigative technique used by the law enforcement authorities. (Section 111 of the CPC) Participation in an organised criminal group is also an offence under SCC as required by the Palermo Convention (Establishing, Masterminding and Supporting a Criminal Group – Section 296 of the SCC).

794. MLA to foreign countries is available in the legislation for the purposes of confiscation. However, the Slovak authorities did not present evidence of any specific rules or concrete arrangements for the disposal of confiscated assets, as required by paragraph 2 of Article 14 of the Palermo Convention.

795. Extradition for all offences is possible on the basis of the CPC. Law enforcement authorities have a range of investigative techniques at their disposal. These include searches for evidence, questioning of suspects and witnesses, and hearing of experts, inspections of sites, searches and seizure.

Implementation of the Terrorist Financing Convention (Articles 2-18, c.35.1 & c. SR. I.1)

796. Slovakia has criminalised TF by virtue of Articles 129, 297 and 419 of the SCC, which is broadly in line with Article 2 of the UN TF Convention. However, there is still the following matter that needs to be addressed with respect to the full implementation of the Convention:

- The acts listed in that paragraph do not seem to cover all of the acts as mentioned in the treaties listed in the annex of the UN TF Convention, and specifically the acts defined in the treaties appearing in the Annex to the Convention. Some of these acts (e. g. acts against fixed platforms) do not seem to appear in the Criminal Code, while others (e.g. hijacking airplanes) appear in other articles of the Criminal Code which are not covered in financing prohibition of Article 419.

797. Apart from these technical shortcomings, in the absence of judicial practice in the Slovak Republic on terrorist financing cases to date, as specified above, it is impossible to evaluate the effectiveness of the system. The case abovementioned in Section 149 gives rise to concerns that the Slovak Authorities are not sufficiently aware of the significance of investigating and prosecuting terrorism financing and do not co-ordinate in these matters, which leads to greater difficulties in investigating and prosecuting these offences.

Implementation of UNSCRs relating to Prevention and Suppression (c. SR.I.2)

798. The UNSCRs 1267 and 1373 relating to the prevention and suppression of the financing of terrorism are implemented in Slovakia within the EU framework by means of EU Regulations and Common Positions, as well as under national legislation through Government Regulation No. 397/2005 Coll. on execution of international sanctions to ensure international peace and security. However, as noted above, Slovakia's national mechanism for giving effect to UNSCRs 1267 and 1373 needs further development. (See. SR III above)

Additional element – Ratification or Implementation of other relevant international conventions

799. The Slovak Republic signed the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (ETS 141) on 8 September 1999 and ratified it on 7 May 2001. The Convention (ETS 141) entered into force for Slovakia on 1 September 2001. The Slovak Republic also signed the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198) on 12 November 2007 and ratified this Convention on 16 September 2008. The Convention entered into force for Slovakia on 1 January 2009.

6.2.2 Recommendations and comments

800. Slovakia ratified the Vienna and Palermo Conventions, as well as the UN TF Convention. The legislation has been amended in order to implement the Conventions; however, the existing legislation does not cover the full scope of these Conventions as stated above and in the individual discussions on R.1 and SR II. Therefore, Slovakia is urged to amend its SCC to fully cover ML and TF offences and thus fully implement the Vienna, Palermo and the UN TF Conventions.

801. Measures still need to be taken in order to properly implement UNSCRs 1267 and 1373.

6.2.3 Compliance with Recommendation 35 and Special Recommendation I

	Rating	Summary of factors underlying rating
R.35	**PC**	• Reservations about certain aspects of the implementation of the Vienna, Palermo and the TF Conventions. • Effectiveness of the implementing the standards in relation to ML and TF gives rise to doubts. • Financing of some of the Acts defined in the treaties appearing in the Annex to the Convention are not criminalised as terrorist financing offence.
SR.I	**PC**	• Financing of some of the Acts defined in the treaties appearing in the Annex to the Convention are not criminalised. • Implementation of UNSCRs 1267 and 1373 is not yet sufficient.

6.3 Mutual legal assistance (R. 36-38, SR. V)

6.3.1 Description and analysis

Recommendation 36 (rated LC in the 3rd round MER)

802. Slovakia was rated Largely Compliant on Recommendation 36 in the 3rd round MER. The report noted that the Slovak Republic had general MLA provisions, covering judicial legal assistance in a way that is not subject to unreasonable conditions. The report identified the lack of information if the authorities were considered best venue mechanisms.

803. Since the adoption of the 3rd round MER, the CCP was amended. The provisions with connection to mutual legal assistance are now in Part V of the CCP, under the title "Legal relation with abroad". Chapter I (of Part V of the CCP) include basic provisions which refer to, *inter alia*, international treaties, reciprocity, protection and use of information, commencement of procedure, etc.

804. Chapter V (of Part V of the CCP) refers to international legal assistance, while division three includes provisions with regard to requests for legal assistance by foreign authorities.

Legal framework

805. As set out in the 3rd round MER, Slovakia is a party to international agreements, such as the 1959 European Convention on Mutual Legal Assistance in Criminal Matters and its Additional protocol and the Strasbourg Convention. In addition, Slovakia signed the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism on 12 November 2007 and ratified it on 16 September 2008. The convention entered into force on 1 January 2009. Slovakia has been a party to the EU Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000 and it's Protocol since 1 October 2006.

806. The Slovak authorities report that they have been finalising the legislative work on transposing the Council Framework Decisions 2005/214/JHA and 2005/783/JHA on the application of mutual recognition to financial penalties and confiscation orders, respectively.[17] In addition, as of 1 April 2010, the Slovak Republic has bilateral co-operation treaties with 38 states.

Widest possible range of mutual assistance (c.36.1)

807. MLA is provided by the Slovak Republic in full accordance with the applicable international treaties. The national provisions of the CCP related to international legal co-operation in criminal matters shall be applied unless an international treaty provides otherwise (Art. 478 of the CCP).

808. According to Section 479 of the CCP, there is a pre-condition of reciprocity, i.e. if the requesting State is not bound by an international treaty, its request shall only be executed by the Slovak authorities if the requesting State guarantees that it would execute a comparable request

[17]The draft law on the implementation of the Council Framework Decision 2005/214/JHA was approved by the Parliament on 1 June 2011 and published in the Collection of Laws as the Act No. 183/2001 Coll. It came into force on 1 August 2011.

submitted by the Slovak authority, and it is not a kind of request whose execution in Chapter I of the CCP is made conditional upon the existence of an international treaty. Furthermore, in case of a request for service of documents to a person on the territory of the Slovak Republic, the compliance with the condition contained above is not examined.

809. Therefore, the Slovak Republic does not apply any additional restrictive conditions for providing mutual legal assistance compared with the conditions set out in the applicable international treaty. The Slovak Republic applies a general rule on Ordre Public defined in Art. 481 of the CCP - the request of a foreign authority can not be executed if its execution would by incompatible with the Constitution of the Slovak Republic or a mandatory rule of the law of the Slovak Republic or if by the execution of the request an important protected interest of the Slovak Republic would be violated.

810. It is concluded that MLA is not made subject to unreasonable, disproportionate or unduly unreasonable restrictive conditions.

Provision of assistance in timely, constructive and effective manner (c. 36.1.1) Clear and efficient processes (c. 36.3)

811. The evaluators, however, were not able to establish the effectiveness of practices regarding time periods given to central authorities, namely, the General Prosecutor's Office and the Ministry of Justice, to evaluate and send the requests for execution, because the Slovak legislation does not provide procedural deadlines for such examination. Though authorities stated that no difficulties have been identified in the timely provision of MLA, they were unable to provide statistics that demonstrate this statement as no such statistics are kept. However, it should be noted that the Slovak authorities were able to provide the evaluators with a letter from the Lord Advocate of Scotland thanking them for their effective and speedy assistance in a high-profile case involving the prosecution of a Slovak national in Scotland.

Provision of assistance regardless of possible involvement of fiscal matters (c. 36.4) Provision of assistance regardless of existence of secrecy and confidentiality laws (c. 36.5) Availability of powers of competent authorities (applying R.28, c. 36.6)

812. No restriction applies with regard to the application of the requirements of criteria 36.4, 36.5 and 36.6. The powers of competent authorities available under R.28 equally apply for use in response to requests for MLA.

Avoiding conflicts of jurisdiction (c. 36.7)

813. With regard to criterion 36.7 of the Methodology, no information was provided on-site on whether Slovakia has considered devising and applying mechanisms for determining the best venue for prosecutions in cases that are subject to prosecution in more than one country. Slovak authorities subsequently reported that they rely on the European conventions to determine how and when cases should be transferred. Slovakia is party to the European Convention on the Transfer of Proceedings in Criminal Matters and the European Convention on Mutual Assistance in Criminal Matters. As a member of the EU, Slovakia is also a member of Eurojust, which is responsible for avoiding such conflicts of jurisdiction. However, these conventions are applicable only between states parties. In the absence of documentation indicating specific arrangements and arrangements with non-European jurisdictions, this criterion cannot be considered to be met.

814. The shortcoming in the incrimination of TF offences in Slovak Law, i.e. lack of criminalisation of individual terrorists' for purposes other than specific acts of terror could negatively impact mutual legal assistance based on dual criminality.

Additional elements (c. 36.8)

815. As noted above, Chapter V (of Part V of the CCP) refers to international legal assistance, while division three includes provisions with regard to requests for legal assistance by foreign authorities. Sections 537 (under the title of "Manner and form of execution of request"), 539 (under the title of "Authorisation of assistance by court"), and 551 (under the title of "Seizure of property") apply the CCP provisions on the request of foreign authorities.

816. The evaluators conclude that the powers of competent authorities required under R. 28 are available for use when there is a direct request from foreign judicial or law enforcement authorities to domestic counterparts.

Recommendation 37 (rated PC in the 3rd round MER)

817. Recommendation 37 was rated *"Partially Compliant"* in the 3rd round MER on the grounds that due to the lack of sufficient incrimination of financing of terrorism in the national legislation, the requirement of dual criminality for extradition would mean that for non-EU countries, some TF offences would not be extraditable. As noted in the 3rd round MER, within the EU borders, the need for dual criminality has been in principle abolished under the European Arrest Warrant.

818. Regarding dual criminality for the criminal offence of financing terrorism (§ 419 of the SCC) and the conclusions of the 3rd round MER, the Slovak authorities point out that the Criminal Code of the Slovak Republic was amended by the Act No. 576/2009 Coll. which entered into force on 1 January 2010. This amendment introduced a separate terrorist financing offence. However, although financing of terrorism has been separately defined as an independent criminal offence, it still does not cover financing individual terrorists for purposes other than specific acts of terror.

819. The Slovak authorities note that in general, dual criminality is not required for providing mutual legal assistance by the Slovak Republic. However, they note that dual criminality is necessary when the taking of evidence requested requires the approval of the court as well as in matters of extradition. They further report that for extradition and those forms of mutual legal assistance where dual criminality is required the Slovak Republic when acting as the requested state considers the dual criminality in general *in abstracto.* Therefore, only the conduct which is a criminal offence under the law of the requesting state is considered and no other conditions based on technical differences are taken into account.

820. However, the evaluators believe that this deficiency is beyond a technical difference and thus the lack of criminalisation of financing of individual terrorists for purposes other that specific acts of terror may have serious implications for MLA, especially in cases when taking evidence requires court approval and in cases of extradition.

Recommendation 38 (rated PC in the 3rd round MER)

821. The 3rd round MER noted that MLA on identification, freezing, seizure, or confiscation of property related to ML, TF or other predicate offences is more problematic than general MLA requests, and stated that uncertainties about the domestic provisions need clarifying in the international context, particularly in relation to forfeiture from third parties. Absence of arrangements for co-ordination of seizure and confiscation actions with other countries as well as for the sharing of confiscated assets between them was one of the other deficiencies identified in the report.

822. According to the Slovak authorities, in respect of listed forms of MLA there is applicable national law based on the CCP and in respect of EU on Act No. 650/2005 Coll. on the execution of

orders freezing property in the sense of Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence. In addition, Sections 60, and 515-521 of the SCC provide for confiscation of property of corresponding value and for arrangements for co-ordinating seizure and confiscation actions with other countries, respectively.

823. In addition, Section 551 of the CCP grants the court, under the conditions specified in an international treaty, the power to order the provisional seizure of movables, immovables, financial assets in bank accounts etc. located in the territory of the Slovak Republic, that are intended to be used to commit a criminal offence, were used to commit a criminal offence or are proceeds of crime, and forfeiture or seizure is expected.

824. The issues mentioned above in Recommendation 3 regarding the inability to forfeit property from third parties also impact this Recommendation, as it may mean that the Slovak Republic is unable to execute a forfeiture request made by another country under certain circumstances.

825. In addition, although some refinements to the SCC and the CCP appear to have improved the legislative framework on confiscation and the MLA regime relating to seizure and confiscation, the Slovak authorities did not present evidence of concrete arrangements for co-ordination of seizure and confiscation actions with other countries or for sharing confiscated assets with them. As a member of the European Union, the Slovak Republic is bound by the Framework Decision on the mutual recognition of confiscation orders, which delineates an asset-sharing arrangement (Article 16), in addition to the membership in Eurojust. Therefore, with regard to European states, the mechanisms appear to be sufficient. However, no information was provided on mechanisms with regard to non-European jurisdictions.

826. Furthermore, absence of detailed statistical data makes judgment about the effectiveness of MLA on confiscation and freezing difficult.

Additional Elements

827. In Slovak law, foreign non-criminal confiscation orders cannot be recognised and enforced in the absence of a bilateral or multilateral agreement.

Special Recommendation V (rated PC in the 3rd round MER)

828. It is concluded above that MLA is not made subject to unreasonable, disproportionate or unduly unreasonable restrictive conditions.

829. Based on indicators, the Slovak authorities reported that the average time period for execution of legal assistance on the basis of a full request for legal assistance was two to three months, while seizures, searches, service of procedural documents and acts executed by means of information technologies are executed without delay. Requests for extradition are handled with the highest level of priority. Provision of documentary evidence or banking data depends on the skills of the providers, but the Slovak authorities provide that no problems have been reported. Requests for assistance addressed to foreign countries are executed within different periods of time depending on the country, and no link was discovered between the type of request and the time taken to respond. The average period of time is 6 to 10 months.

830. In addition, the absence of incrimination of financing of individual terrorists' for purposes other than specific acts of terror may continue to limit the MLA regime regarding TF.

831. It was determined that the Slovak authorities note that in general, dual criminality is not required for providing mutual legal assistance by the Slovak Republic. However, they note that dual criminality is necessary when the taking of the evidence requested requires the approval of the court as well as in matters of extradition. They further report that for extradition and those forms of mutual legal assistance where dual criminality is required the Slovak Republic when acting as the requested state considers the dual criminality in general *in abstracto*. Therefore, only the conduct which is a criminal offence under the law of the requesting state is considered and no other conditions based on technical differences are taken into account.

832. However, as noted above, the evaluators believe that this deficiency is beyond a technical difference and thus the lack of criminalisation of financing of individual terrorists for purposes other than specific acts of terror may have serious implications for MLA, especially in cases when taking evidence requires court approval and in cases of extradition.

833. It was noted that the Slovak authorities did not present evidence of concrete arrangements for co-ordination of seizure and confiscation actions with other countries or for sharing confiscated assets with them, and this issue is relevant also to offences of financing of terrorism, terrorist acts and terrorist organisations.

Additional element under SR V (applying c. 36.7 & 36.8 in R. 36, c.V.6)

834. With regard to c. 36.8 the evaluators concluded that the powers of competent authorities required under R. 28 are available for use when there is a direct request from foreign judicial or law enforcement authorities to domestic counterparts.

835. With regard to c. 38.6, as the Slovak Authorities specified, in Slovak law, foreign non-criminal confiscation orders cannot be recognised and enforced in the absence of a bilateral or multilateral agreement.

Recommendation 30 (Resources – Central authority for sending/receiving mutual legal assistance/extradition requests)

836. As of 31 December, 2010, 12 prosecutorial positions were staffed and one additional vacancy existed in the International Department of the General Prosecutor's Office. This department also includes five civil servants and two translators. In the eight regional prosecution offices, there are a total of 24 prosecutors dealing with these issues. In addition, there are one or two prosecutors in the district prosecution offices specialising in legal co-operation with foreign countries. The Ministry of Justice contains an additional six employees dealing with MLA and extradition requests, including European arrest warrants. As of 17 May 2011, there were 231 pending requests for MLA and 916 pending requests for extradition, including European Arrest Warrants.

Recommendation 32 (Statistics – c. 32.2)

837. The Slovak authorities provided the following statistics concerning mutual legal assistance:

Request for legal assistance sent to foreign country

Title of act/dead line (months)	Questioning of witness/injured party	Documentary evidence and search for other data	Bank data	service	Expert opinion	total
2005	LI/10, AT/8, CZ/8,	LI/1, AT/8,CZ/8				10

	DE/8, S/8	DE/8, SE/8				
2006	DE/8, DE/4	DE/8				3
2007	AT/8 , AT/5, HU/4	US/ 1				4
2008	CZ/5,CZ/5, DE/3, DE/8, AT/5, IT/8,	AT/1, CZ/5		DE/8-2x		10
2009	CZ/4, CZ /2, CZ/5, CZ/3, AT/3, AT/8, AT/5, IT/8, IT/12, IT/10+, UK/18, US/11, US/12+, PL/8, HR/3, EE/6, DE/10+	CZ /4, IT/8, IT/8 AT/5, HR/7 US/12+	US/12+ JE/18		CZ/1 HR/3	27
2010	DE/4, DE/6+, DE/8+ IT/9+, IT/8+, IT/7+ AT/1, AT/3, AT/4+ ČZ/2, CZ /3, CZ /4 CZ /7,CZ /2, CZ/3+ PL/4, RU/5+,LT/5+ CH/10+, CH/7+ UA/2+, US/4+ CY/3+, JP/2+	CZ /4,CZ /4, CZ/3, CZ/3+,HU/4+, UA/2+ ES/4, BE/2+, PL/3, HU/4, US/4+, CY/3+, JP/2+, DK/3+	CY/3+, IM/1+, GG/1+			41

Requests received by Slovakia as executing country – data are as follows:

Money Laundering:
2008 - 2x (questionings of witnesses, seizure of documentary evidence and banking information)
2010 - 6x - 1x GE, 1xUSA – 11x witness questioning, also seizure of documentary evidence and banking information,
2x extradition of person

Financing of terrorism:
2009 - 1x (freezing of accounts – 5x, 10x witness questioning, home search, search of other premises, banking data, documentary evidence)
2010 - 1x (2x witness questioning, banking information, documentary evidence).

838. In general, the Ministry of Justice of the Slovak Republic keeps statistics on the number of requests for MLA and extradition. However, the statistics provided to the evaluators are not comprehensive and adequately detailed both in general terms and specifically on ML/TF offences. However, according to the Ministry of Justice, as of 17 May 2011, there were no requests relating to money laundering, predicate offences to money laundering or terrorist financing.

839. The Annual Activity Report of the Public Prosecution Service includes statistics on MLA, based on which the Slovak authorities were able to provide the following information:

Total number of cases

	Central Judicial Authority Int. Dep. GPO*	Competent Judicial Authority County Pros. Office	Competent Judicial Authority District Pros. Office	Eurojust	European Judicial Network
2006	1528	3086	2829	23	15
2007	1501	2545	3348	33	66
2008	1728	2332	4108	47	37
2009	1754	2459	4870	34	52
2010	1873	2816	5546	33	39

*General Prosecution Office in the position of Central Judicial Authority

Transfer of Criminal Proceedings (including Criminal Complaints)

	Criminal Proceedings		Criminal Complaints			
	Transferred to	Accepted from	Transferred to		Accepted from	
			GPO*	C&D PO**	GPO*	C&D PO**
2006	136	80	170	27▪	345	608
2007	154	93	174	31▪	373	713
2008	155	148	221	36▪	475	917
2009	124	100	287	35▪	457	803
2010	141	112	354	40▪	578	900

* General Prosecution Office in the position of Central Judicial Authority

** County and District Prosecutions Offices in the position of Competent Judicial Authority – direct communication between competent judicial authorities of requesting and requested party

▪ County and District Prosecutions Offices in the position of Competent Judicial Authority – direct communication between competent judicial authorities of requesting and requested party available only with CZ and PL.

Mutual Legal Assistance - SK - Requested Party

	Request addressed to								
	GPO*	C&D PO**	Total	Hearing, Interrogation	Delivery of procedural documents	House search and similar	Confiscation	Documents and other information	Overall number of acts required
2006	140	814	954	516	301	14		103	1446
2007	336	652	986	667	314	14		43	1182
2008	358	1014	1372	999	410	9		194	1710
2009	412	1134	1556	1037	371	19	18	209	1814
2010	323	1387	1710	1259	313	9		193	1961

* General Prosecution Office in the position of Central Judicial Authority

** County and District Prosecutions Offices in the position of Competent Judicial Authority – direct communication between competent judicial authorities of requesting and requested party

Mutual Legal Assistance - SK - Requesting Party

	Requesting by								
	GPO*	C&D PO**	Total	Hearing, Interrogation	Delivery of procedural documents	Confiscation	Documents and other information	Other acts required	Overall number of acts required
2006	283	1163	1446	1123	98		204	113	
2007	336	652	986	667	314	10	43	37	1776
2008	358	1014	1372	999	410		194	59	2675
2009	412	1134	1556	1037	371		209	115	2981
2010	323	1387	1710	1259	313		193	354	3631

* General Prosecution Office in the position of Central Judicial Authority

** County and District Prosecutions Offices in the position of Competent Judicial Authority – direct communication between competent judicial authorities of requesting and requested party

Mutual Legal Assistance - Extradition

	Extradition of the accused/offender to a foreign country		Requesting a suspect/accused/offender to be brought from foreign country	
	International Arrest Warrant	European Arrest Warrant	International Arrest Warrant	European Arrest Warrant
2006	15	32	33	35
2007	2	96	34	44
2008	-	108	20	54
2009	6	125	11/10*	59/57*
2010	7	137	5	61/59*

Note: * notions implied by prosecutors/accepted by courts

Effectiveness and efficiency

840. There seems to be sufficient international co-operation, although it is hard for the evaluators to form a full picture of the situation in light of the lack of specific statistics regarding MLA requests.

6.3.2 Recommendations and comments

841. The issues with the legal definition of financing of terrorism negatively impacts the MLA regime, since certain forms of legal assistance requiring dual criminality cannot be provided for terror financing that is not covered (i.e. financing of individuals terrorists for purposes other than specific acts of terror).

842. In addition, the inability to forfeit property from third parties may limit the ability of the Slovak authorities to respond to foreign requests for confiscation and forfeiture under certain circumstances.

843. The Slovak authorities have not provided evidence of concrete arrangements for co-ordination of seizure and confiscation actions with other countries or for sharing confiscated assets with them, other than the arrangements that exist for other European jurisdictions by virtue of the Slovak Republic's membership in Eurojust and the Framework Decision. Nor was information provided on-site on whether Slovakia has considered devising and applying mechanisms for determining the best venue for prosecutions in cases that are subject to prosecution in more than one country.

6.3.3 Compliance with Recommendations 36 to 38 and Special Recommendation V

	Rating	Summary of factors relevant to s.6.3. underlying overall rating
R.36	**LC**	• Lack of criminalisation of individual terrorists' for purposes other than specific acts of terrorism could negatively impact mutual legal assistance based on dual criminality. • No information was provided on whether the authorities have considered best venue for prosecution in cases subject to prosecution in more than one country, other than as provided under the membership in Eurojust.
R.37	**LC**	• The limitations in the definition of the financing of terrorism may limit the ability of the Slovak Republic to provide MLA.
R.38	**PC**	• The limitations in the definition of the financing of terrorism may limit the ability of the Slovak Republic to provide MLA. • Difficulties in forfeiting property from third parties may limit the ability of the Slovak Republic to provide MLA. • No evidence of concrete arrangements for co-ordination of seizure and confiscation actions with other countries or for sharing confiscated assets with them, other than those provided under the Framework Decision applicable for EU Member States. • Absence of adequately detailed statistics makes judgment on effectiveness difficult.
SR.V	**LC**	• The limitations in the definition of the financing of terrorism may limit the ability of the Slovak Republic to provide MLA.

6.4 Other Forms of International Co-operation (R. 40 and SR.V)

6.4.1 Description and analysis

Recommendation 40 (rated LC in the 3rd round MER)

Legal framework

844. Section 28 of the AML/CFT Act provides for the legal basis for international co-operation of the FIU with the respective authorities of the Member States of the EC, and with authorities of other states to the extent and upon the terms laid down in international treaty binding on the Slovak Republic or on the grounds of the non-contractual reciprocity principle. The FIU may also co-operate with international organisations involved in the area of the prevention and detection of legalisation of proceeds of criminal activity and terrorist financing.

845. Slovak law enforcement authorities are entitled to co-operate with foreign counterparts according to Article 77a of the Act on Police Force, which states that the Police force co-operate with the police forces of other states, with international police organisations, international organisations and organisations officiate on the territories of other states particularly by the exchanging of information, exchanging of liaison officers, or other forms.

846. The FIU, as an integral part of the Police force uses opportunities to exchange information laid down in both the AML/CFT Act and the Act on Police Force.

847. Customs Administration is entitled to co-operate with customs administrations of other countries, as well as with international organisations according to Section 4 of the Act on State Administration bodies in the field of Customs and on Amendments and Supplements to some Acts, Coll. 652/2004. This section states that the Customs Administration co-operates with foreign counterparts to the extent and under the terms stipulated by legally binding acts of the European Communities and European Union, international agreement or treaty between the parties concerned. Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and co-operation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters is used for mutual co-operation between administrative authorities of the member states of the EU. The Convention on mutual assistance and co-operation between customs administrations, so called Naples II Convention, is commonly used in the international co-operation.

Wide range of international co-operation (c.40.1); Provision of assistance in timely, constructive and effective manner (c.40.1.1); Clear and effective gateways for exchange of information (c.40.2), Spontaneous exchange of information (c. 40.3)

FIU

848. The FIU performs information exchange through the encrypted electronic security network ESW (Egmont Secure Web) created within the Egmont Group. The Slovak FIU became a member of the EGMONT Group in June 1997. Information exchange is done also in the framework of the FIU.NET, established in EU countries. The Slovak FIU joined this network in 2004.

849. The FIU has signed MOUs with the FIU of Belgium, the Czech Republic, Slovenia, Poland, Ukraine, Monaco, Australia and Albania. International information exchange of the FIU can be illustrated by the following statistics:

2007:
- 82 requests from foreign FIUs, all replied by the Slovak FIU,
- 47 requests sent to foreign FIUs,
- 88 spontaneous information disseminated to foreign FIUs by the Slovak FIU.

2008:
- 62 requests from foreign FIUs, all replied by the Slovak FIU,
- 74 requests sent to foreign FIUs,
- 174 spontaneous information disseminated to foreign FIUs by the Slovak FIU, the Slovak FIU received 23 pieces of feedback,
- 7 spontaneous information received from foreign FIUs.

2010:
- 84 requests from foreign FIUs, all were replied by the Slovak FIU,
- 145 own requests sent to foreign FIUs,
- 420 own spontaneous information disseminated to foreign FIUs by the Slovak FIU, the Slovak FIU received 74 pieces of feedback,
- 27 spontaneous information received from foreign FIUs.

Authorities reported that the FIU responds to the requests without undue delays, depending on the content of the request, in 30 days at the latest, and just in exceptional cases in longer period if another institution is required to involve in provision of assistance.

850. The FIU is able to provide the information to foreign counterparts both spontaneously and upon a request which is regularly done in practice. Slovak authorities informed evaluators that in the first half of year 2010 the FIU sent 186 cases spontaneously providing foreign counterparts with information.

Supervisory authorities

851. The information given on R.40 in the 3rd round MER were fairly accurate on the date of the on-site visit. The NBS – as the sole financial market regulator – still has a full range of powers to co-operate with foreign supervisory bodies for purposes of consolidated supervision and to exchange information. As the Financial Market Authority has become a part of the National Bank of Slovakia, the NBS is now subject to all international memoranda and other agreements, as a successor to the Financial Market Authority. The powers to co-operate on an international level arise now directly form paragraph 3 of Article 1 letter (e) of the FMS Act. There are still 9 bilateral memoranda of understanding signed by the NBS for the purpose of exchanging information. The NBS is also a party to 2 multilateral MoUs (the IOSCO MoU and CESR MoU), which allows them to exchange information with all EU Member States and 72 Member States which have signed the IOSCO MoU. No statistics were however provided to allow the evaluation team to assess the effectiveness of the co-operation.

852. Under Section 27 of the AML/CFT Act the FIU can co-operate with the respective authorities of the Member States and the European Commission, the Council of the European Union and the Secretariat of the Council of the European Union, especially in the exchange and verification of information in the field of AML/CFT. This is also true for the co-operation with other states to the extent and upon the terms laid down in international treaty binding on the Slovak Republic or on the grounds of the non-contractual reciprocity principle. The FIU may also co-operate with international organisations involved in the said area. As there are no legal limitations the evaluators believe that this provision provides sufficient legal grounds for the FIU's co-operation in its capacity as a supervisory authority.

Law enforcement authorities

853. Slovakia is a member of following global and regional police co-operation organisations and initiatives:

- Interpol,
- signatory to the Schengen Agreement,
- European Union Law Enforcement Agency (Europol),
- Salzburg Forum,
- United Nations Drug Control Programme,
- International Police Agency,
- European Network of Forensic Science Institutions,
- Traffic Information System for Police.

854. Police authorities directly exchange information with foreign counterparts using Interpol and Europol channels. However, no statistical data has been provided to show the effectiveness of this co-operation.

855. Statistical data on information exchange provided by National Bureaux of Europol and Interpol Slovakia for period 01.01.2010 – 31.12.2010 is as follows:

Interpol
- requests received – 29,381,
- requests sent out – 19,237.

856. Statistics on information exchange through Europol are regularly published by the Europol office.

857. The following table shows statistics on requests for information provided by liaison officers of Slovak Police force situated in foreign countries:

Liaison Bureau at Embassies of the Slovak Republic	**Requests from units of Ministry of Interior and police of a foreign country**		**Requests from units of Ministry or Police Force**		**Requests from other subject of a foreign country or Slovakia**		**Total number**	
	Replied	**Pending**	**Replied**	**Pending**	**Replied**	**Pending**	**2010**	***2009***
Beograd	5	0	36	2	11	0	54	*51*
Budapest	41	0	84	9	7	0	141	*142*
Bucharest	23	2	44	2	12	0	83	*87*
Kyiv	4	2	30	7	4	2	49	*63*
London	48	0	54	0	21	0	123	*99*
Moscow	14	0	44	4	21	0	83	*79*
Prague	35	10	117	0	19	0	181	*182*
Rome	22	0	57	3	2	0	84	*70*
Warsaw	36	0	82	6	13	0	137	*92*
Vienna	14	0	78	0	14	0	106	*87*
Zagreb	9	0	48	3	15	0	75	*68*
Total	**251**	**14**	**674**	**36**	**139**	**2**	**1116**	***1054***

	265	**710**				

Customs authorities:

858. International co-operation and information exchange of Customs Administration is performed in the framework of abovementioned international instruments in a timely, constructive and effective manner, as advised by the authorities. However, no statistics has been provided to demonstrate this statement. International co-operation is performed on the basis of the requests, spontaneous assistance and through the Customs Information System (CIS). Within the EU, law enforcement sensitive information is shared between customs both via formal and informal channels (bearing in mind the time factor in the latter case). An important element of exchanging cash control related information is the platform set up by the EU Commission which is the Cash Control Working Group with participants of customs officials of every EU Member State, convened on a regular basis. The RIF system is accessible to all EU Member States' customs authorities thus ensuring the timely and prompt access to all cash control related suspicious cases, trends. Information on suspicious cash movement are recorded and stored in the RIF system, which is accessible to all customs services throughout the EU. In case of third countries, information can be exchanged on request by competent authorities of either third countries or their Slovak counterpart. Slovak Customs Authorities regularly receive information from other member states about new trends and seizures in the field of cash transfers. This co-operation is informal but very useful. Slovak Customs Authorities have participated in the international control operations focused on the illegal money transfers, money laundering and terrorist financing. They reported that they had involved in the operation ATLAS, which focused on the physical cross-border transportation of currency or bearer negotiable instruments and took place in October 2009 at international airports.

Making inquiries on behalf of foreign counterparts (c.40.4), FIU authorised to make inquiries on behalf of foreign counterparts (c. 40.4.1), Conducting of investigation on behalf of foreign counterparts (c. 40.5)

FIU

859. The Slovak FIU does not differentiate international investigations and information requests from national ones. Therefore, the FIU can make all inquires that it usually makes in its own work, also in responding the requests from foreign FIUs. This is regularly done in practice, which is confirmed by other FIUs' responses to the query on international co-operation, which was sent by MONEYVAL prior to the on-site visit.

Supervisory authorities

860. The NBS, as a general rule, has access to all relevant information which may be important in any way in conducting their supervision (i.e. on the basis of Article 3 of the FMS Act). There are no legal impediments for the NBS to request any information (on the basis of the provisions of Slovak Law), when the foreign counterpart requested so (there are also specific provisions in this particular matter for instance in the Act on Banks).

Law enforcement authorities

861. Slovak authorities referred to paragraph 1 of Article 77a of the Act on Police Force with regard to conducting investigations on behalf of foreign counterparts. The mentioned paragraph provides for the legal basis for international co-operation of law enforcement agencies stating that the Police

Force co-operates with foreign law enforcement authorities especially by exchanging information and by other forms co-operation. This is considered to include also starting investigation on behalf of foreign counterparts.

Customs authorities

862. On the basis of foreign requests Slovak Customs Administration can provide any action allowed by national legislation related to customs authorities, mainly the Act No 652/2004 on State Administration Bodies in the Field of Customs and on Amendments and Supplements to Some Acts. According this act Slovak Customs Administration can make inquires to companies, state authorities and other relevant bodies.

No unreasonable or unduly restrictive conditions on exchange of information (c.40.6)

Law enforcement authorities – FIU

863. According to paragraph 9 of Section 69da of the Act on Police Force the competent law enforcement authorities, including the FIU, may refuse to provide information or intelligence only if there are factual reasons to assume that the provision of the information or intelligence would harm essential national security interests of the Slovak Republic, jeopardise the success of a current investigation or a criminal intelligence operation or the safety of individuals, clearly be disproportionate or irrelevant with regard to the purposes, for which it has been requested.

864. Where the request pertains to an offence punishable by a term of imprisonment of one year or less under the Slovak law, the competent law enforcement authority may refuse to provide the requested information or intelligence.

865. Section 69(da) deals with the international co-operation and information exchange between Slovak Police Force and other member states of the EU. There are no other restrictive conditions with regard to other countries or EU Member States.

Supervisory authorities

866. When assessing the legal provisions of the FMS Act there could not be found any unreasonable or unduly restrictive conditions on exchange of information by the NBS. It is worth to bear in mind that the specific conditions of co-operation are set out in respective memoranda of understanding, which also do not have such provisions. The said memoranda are based on the framework provided by the Basel Committee, and multilateral memoranda are the once of CESR (currently ESMA) and IOSCO.

Customs authorities:

867. Only restrictions that are applied in performing international co-operation of Customs Administration are related to the Act No. 428/2002 on Protection of Personal Data. Secret and confidential data is processed in compliance with the National Act No 215/2004 Coll. on protection of classified information. No unreasonable or unduly restrictive conditions on exchange of information are applied in customs international co-operation.

Provision of assistance regardless of possible involvement of fiscal matters (c.40.7) Provision of assistance regardless of existence of secrecy and confidentiality laws (c.40.8)

Law enforcement authorities - FIU

868. Since no restrictive conditions are prescribed, the FIU and other law enforcement agencies are able to provide assistance irrespective of possible involvement of fiscal matters and regardless of existence of secrecy and confidentiality laws

Supervisory authorities

869. There are no provisions in law, or in any of the binding multilateral or bilateral MoUs signed by the NBS, which could be interpreted as prohibiting assistance, when the case would be on fiscal matters. There are also no provisions in the Slovak legislation or in any of the binding multilateral or bilateral MoUs signed by the NBS, which could be interpreted as prohibiting assistance on the grounds of laws that impose secrecy or confidentiality requirements on financial institutions.

Safeguards in use of exchanged information (c.40.9)

FIU

870. Information received from foreign FIUs is inserted into the internal autonomous database of the Slovak FIU. The information is disseminated to third parties only on the bases of written consent given by the foreign FIU. All legal and other safeguards already mentioned with regard to use of information received by the FIU apply here as well.

871. All the information provided to the Slovak FIU is only for intelligence purposes. If the provided information should serve as evidence in any formal proceedings then an international rogatory letter is required.

Supervisory authorities

872. All of the MoUs, which were in the scope of this assessment, place a great deal of emphasis on the issue of safeguards to ensure that information received by competent authorities is used only in authorised manner. The said provisions are deemed to be sufficient to fulfil the requirements of criterion 40.9.

Law enforcement authorities

873. The safeguards in the use of internationally exchanged information by law enforcement authorities are stipulated in Sections 69 of the Act on Police Force that deals with processing of personal data, wording of which is taken from Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the EU Member States.

874. Information exchanged by law enforcement authorities is ensured either by regular post provided by internal couriers of the Police Force or by the certified secured e-mail communication channel of the Police Force. Any information sent by the regular post by couriers of the Police Force is properly enveloped and closed. Secured e-mail communication channel meets all security requirements standards of secure communication.

875. The General Prosecutor Office of the Slovak Republic has protected links to Eurojust and some other international institutions, which are used for transfer of protected data. Similar situation is on the level of police co-operation and inter-ministerial co-operation with foreign partners.

Customs authorities:

876. Provisions of the Act No. 428/2002 on Protection of Personal Data and the Act No 215/2004 Coll. on protection of classified information are used as safeguards to ensure that information received by customs office is used only in an authorised manner

Additional elements – Exchange of information with non counterparts (c.40.10 and c.40.40.1); Exchange of information to FIU by other competent authorities pursuant to request from foreign FIU (c.40.11)

FIU

877. The Slovak FIU regularly exchange information only with foreign FIUs. The FIU is able to obtain information from other competent bodies, on the basis of a request made by a foreign FIU, which is done in practice.

Supervisory authorities

878. As mentioned above there are provisions in law which allow the NBS to exchange information with supervisors, which are not party to any of the signed bilateral or multilateral MoUs. The evaluation team was however not presented with any case indicating that such request was made, and what the extent of it was and the extent of information divulged by both parties.

Law enforcement authorities

879. Law enforcement authorities of the Police Force are authorised to co-operate based on Section 77a of Act No. 171/1993 Coll. on the Act on Police Force also with non-counterparts either indirectly using traditional police channels (Interpol, Europol, liaison officers) or directly when there are agreements to allow for such co-operation. As provided in Section 77a the Police Force shall co-operate with the polices of other states, with international police organisations, international organisations and organisations acting in the territories of other states particularly in the form of information exchange, liaison officers exchange, eventually in other forms. Also, the Ministry may, for the performance of tasks of the Police Force also outside the territory of the Slovak Republic, delegate the police officers to the international police organisations, policies of other states, international peace missions, international operations of the civil crisis management or after agreement with the MFA of the Slovak Republic to diplomatic missions of the Slovak Republic or to international organisations.

International co-operation under SR.V (applying 40.1-40.9 in R.40, c.V.5) (rated PC in the 3rd round MER) - Additional element under SR.V – (applying 40.10-40.11 in R.40, c.V.9)

880. All measures taken in international co-operation with respect to money laundering could be taken in respect of terrorism financing as well.

Recommendation 32 (Statistics – other requests made or received by the FIU, spontaneous referrals, requests made or received by supervisors)

881. In 2009, the Slovak FIU co-operated with 61 counterpart FIUs, members of Egmont Group and 5 counterpart FIUs associated within the system of FIU.NET. The most intense co-operation is realised with the FIU of the Czech Republic, Hungary, Austria, Germany, Cyprus, Italy, the Russian Federation, Ukraine, the United Kingdom and the USA.

882. The following table shows statistics of international information exchange for the year 2009.

FIU	Request for information	Information/request from a foreign FIU	Consent to disseminate information from UTs to LEA
Australia	0	1	1
Belgium	3	2	1
Bahamas	1	0	0
Belize	2	1	0
Belorussia	0	1	1
Bosnia - Herzegovina	0	1	0
British Virgin Islands	1	0	0
Bulgaria	1	0	1
Costa Rica	0	2	0
Cyprus	11	1	1
Czech Republic	12	20	14
Montenegro	0	4	0
Denmark	1	1	0
Estonia	1	4	2
Finland	0	2	0
France	2	1	0
Greece	1	1	0
Gibraltar	1	0	0
the Netherlands	2	0	0
Hong Kong	1	0	0
Croatia	1	1	1
India	0	1	0
Ireland	0	0	0
Isle of Man	2	0	2
Israel	0	1	0
Canada	0	0	0
Lebanon	0	0	0
Lichtenstein	3	0	0
Lithuania	1	0	0
Luxemburg	1	1	0
Latvia	3	1	0
"The former Yugoslav Republic of Macedonia"	0	1	0
Hungary	19	10	18
Malta	1	0	0
Marshall Islands	1	0	0

Mexico	0	1	0
Moldova	0	1	0
Monaco	3	0	1
Germany	35	3	17
Nigeria	0	2	0
New Zealand	1	0	2
Islands Turk and Caicos	0	1	0
Panama	1	0	0
Poland	4	9	3
Portugal	0	0	0
Austria	8	1	6
Romania	14	1	4
Russian Federation	7	1	1
Slovenia	0	0	0
United Arab Emirates	0	0	0
Sri Lanka	0	1	0
Serbia	0	2	0
Spain	5	0	0
Sweden	2	0	1
Switzerland	3	1	3
Taiwan	0	0	0
Italy	5	0	3
Turkey	0	1	0
Ukraine	7	7	4
the USA	4	0	1
Venezuela	0	3	0
the United Kingdom	12	3	1
Total	**183**	**96**	**89**

883. Between 1 January 2010 and 30 June 2010 the FIU received 46 requests from foreign FIUs and sent 84 requests for providing information to foreign FIUs. No statistics for previous years have been provided.

884. The authorities reported that the FIU sent 16 requests and spontaneously provided information in relation to TF cases in 2009.

885. The evaluation team was not presented with any statistics on international co-operation undertaken by the NBS or by the FIU on supervisory matters. It is advisable for the NBS to have such detailed statistics

Effectiveness and efficiency

FIU

886. According to statistics provided for 2009 and 2010, as well as information provided by counterpart FIUs, it seems that the Slovak FIU exchanges information at the international level very effectively. This can be confirmed also by the practice of the FIU to collect and share with foreign FIUs all information available to it in domestic investigations. In considerations regarding R.26 above, it was mentioned that the FIU has direct or indirect access to a variety of databases.

Supervisory authorities

887. Though the legal framework for the international co-operation is in place, the statistics are lacking which does not allow the full assessment of the effectiveness of the international co-operation by the NBS. The evaluation team was not advised on legal provisions allowing the MoF for the international exchange of information in respect of their supervisory powers. No such provisions can also be found in the Act on Gambling.

888. Authorities stated that the FIU Slovakia may co-operate with foreign FIUs also concerning supervision related matters. They further reported that it has not been requested by any foreign FIU to make use of its supervising function so far.

Law enforcement authorities

889. Although it appears to evaluators that law enforcement agencies have sufficient basis and effective gateways for international information exchange and that these are used in practice, no statistics have been made available to the evaluation team in order to demonstrate the effectiveness of this co-operation.

6.4.2 Recommendation and comments

FIU - Law enforcement authorities- Supervisory authorities

890. The Slovak authorities appear to have sufficient powers to enable them to provide different forms of assistance, information and co-operation without undue delay or hindrance.

891. The responses received to the MONEYVAL's standard enquiry on international co-operation which was sent to the MONEYVAL and the FATF members received generally a positive response. Particularly the FIU's co-operation and exchange of information at the international level is well regarded.

892. Due to the lack of detailed statistics it was not possible to assess how effectively the Slovak authorities were responding to international co-operation requests and therefore, it is recommended that procedures are put in place to centrally record and monitor all international co-operation requests on matters related to ML and TF.

Supervisory authorities

893. It is advisable for the NBS to keep detailed statistics on their international co-operation, as there are none whatsoever.

894. The Slovak authorities should consider the feasibility of international exchange of information in respect of gambling supervision conducted by the MoF.

6.4.3 Compliance with Recommendation 40 and SR.V

	Rating	Summary of factors relevant to s.6.5 underlying overall rating
R.40	**LC**	• Lack of detailed statistics undermines the assessment of effectiveness. (for supervisory authorities)
SR.V	**LC**	• Lack of detailed statistics undermines the assessment of effectiveness.

7 OTHER ISSUES

7.1 Resources and Statistics

7.1.1 Description and analysis

Recommendation 30 (rated PC in the 3rd round MER)

895. Recommendation 30 was rated *"Partially Compliant"* in the 3rd round MER based on the need for more resources for the FIU (particularly for supervision) and the need for more staff and training for prudential supervisors. Requirement of more training and guidance for the law enforcement was another underlying factor for this rating.

The FIU

896. Overall, the FIU is well structured, professional and appears to be operating effectively. Out of 37 staff eight police officers including the head of department deals with the analysis of unusual transaction reports. Plans for further improving the FIU's IT system is reported to have been approved by the Government. Budget for the FIU has steadily increased between 2006 and 2010. However as noted above the evaluation team believe that additional measures should be taken by the authorities to adequately fund and staff the FIU particularly in order to reinforce its analysis capacities. The FIU's staff holds certificates issued by the National Security Bureau. They are obliged to abide by confidentiality rules as set out by the AML/CFT Act. Further details are given in section 2.5 above.

Law enforcement and prosecution agencies

897. The police and prosecutors seemed to be adequately resourced and trained. However, there were concerns of the level of resources devoted to the investigation and prosecution of ML offences particularly in a wide range of major and more serious predicate offences perpetrated by organised crime or others for pure economic gain, and the level of priority given to such cases. This was reflected in the low number of ML convictions as well as the low number of application of provisional measures and confiscations. Further details are given in section 2.1 above.

Supervisors

898. With regard to financial sector supervisors, the NBS has sufficient resources, and the employees seem to be well trained. It is, however, important to provide TF trainings to employees engaged in AML/CFT issues.

899. The FIU staff designated to conduct on-site visits is also well trained and experienced. However, the resources of the FIU still are not sufficient enough to deal with the scope of supervision prescribed by the AML/CFT Act. The FIU employs 37 police officers and one civil servant, and the part responsible for controls employs six people (plus one person designated as a head of this office).

900. No mechanism exists in place, which seems to regard itself responsible for the monitoring of the implementation of SR III requirements by financial institutions and DNFBPs.

901. As mentioned above, the Ministry of Finance supervising the gambling sector. It is of concern that the MoF is not sufficiently staffed to deal with the responsibilities of conducting on-site inspections. Further details of resources in supervision are given in sections 3.2 and 3.7 above.

Policy makers

902. Apart from the general data received, the Slovak authorities have not provided any details on the allocation of other resources used to set up and maintain the AML/CFT system on the policy level. Thus it was not demonstrated that requirements under Recommendation 30 for policy makers of competent authorities are met.

903. There is no effective mechanism in place for the supervision or monitoring of those NPOs which account for a significant portion of the financial resources under the control of the sector and a substantial share of the sector's international activities.

904. Regarding the national and international co-operation, it appears that this is seen as a priority and that there is an adequate level of resourcing applied. Further details are given in section 6 above.

Recommendation 32(rated PC in the 3rd round MER)

905. Recommendation 30 was rated *"Partially Compliant"* in the 3rd round MER because of the following factors:

- More detailed statistics on ML investigations, prosecutions and convictions are required and needed also to be communicated to the FIU;
- More detailed statistics required in relation to freezing under UNSCRs outside of the banks and on confiscation orders;
- More statistics are required on supervision showing the nature of problems in AML/CFT implementation and more detailed statistics on judicial co-operation.

906. As noted above, Section 27 of the new AML/CFT Act authorises the FIU to keep statistics covering, *inter alia*, the number of cases submitted by the FIU to law enforcement authorities, the number of persons prosecuted or convicted of legalisation of proceeds from criminal activity, the value of seized or confiscated property, and to publish a summary review of that statistical data in an annual report. The same section also authorises it, for the purposes of keeping statistics, to require public authorities to supply all necessary documents and information to the FIU. Though this obligation under Section 27 does not cover keeping of statistics relating to TF cases, the authorities report that the FIU, in practice, collects statistics on the disseminated information related to TF.

907. With regard to the investigation and prosecution of ML and TF offences, in the course of the evaluation the evaluators have been provided with different sets of statistics, each of which was presented as being more up-to-date and accurate. However, there were inconsistencies amongst those various statistics and thus, the evaluators came to the conclusion that the manner of calculating of those statistics is not fully coherent. This has made it difficult for the evaluators to regard the statistics as clear indications of the actual scope of legal proceedings. Similarly, the statistics provided related to the freezing and confiscation were not coherent and sufficiently meaningful. No statistics is kept relating to freezing and confiscation of proceeds of predicate offences. Further details are given in sections 2.1 and 2.3.

908. The FIU maintains comprehensive statistics on unusual transaction reports, on cases opened and disseminated to competent authorities with breakdown of which authorities are provided with information, on international co-operation with foreign FIUs, on transactions postponed after

receiving UTRs, on reports received form Customs on cash transfers and on feedback received from law enforcement on results of the cases disseminated by the FIU.

909. The issue of concern regarding statistics kept by the FIU is that the statistics maintained and provided to evaluators, do not appear to concentrate on ML or TF cases, but on all criminal offences equally. Further details are given in section 2.5 above.

910. Comprehensive statistics is maintained by the FIU and the Customs regarding declarations made by travellers as described in Section 2.6. However, there are no statistics on cases of false declarations or failure to declare, nor on suspicious cases of possible money laundering or terrorism financing.

911. Overall, the statistics provided by the NBS and the FIU relating to the supervision of reporting entities were comprehensive and detailed enough. The evaluation team, however, was not given any statistics on international co-operation and requests for assistance from foreign supervisory authorities. In addition, no detailed and comprehensive statistics with regard to gambling sector supervision, as required by R.32, has been provided by the MoF. Further details are given in sections 3.8 and 4.3.

912. There is no proof whatsoever of any collective review of the Slovak system done at any other level. The IIGE has been mandated to work on "unification and consolidation of process of collecting the statistical data related to ML and TF kept by the Ministry of Interior of the Slovak Republic, the General Prosecutor's Office and the Ministry of Justice of the Slovak Republic", but authorities have not provided the evaluators with any of the results in this regard.

913. The Ministry of Justice of the Slovak Republic keeps statistics on the number of requests for MLA and extradition. The statistics provided to the evaluators are, however, not comprehensive and adequately detailed both in general terms and specifically on ML/TF offences. Further details are given in section 6.3.

7.1.2 Recommendation and comments

Recommendation 30

914. Slovak authorities could give more specific training on ML and TF offences, and the seizure, freezing and confiscation of property that is the proceeds of crime or is to be used to finance terrorism to police, prosecutors and judges.

915. More resources and staff should be dedicated to the FIU for its activities in the supervision field and for its performance of a more effective national co-ordination role.

916. More staff and resources should be provided to the Ministry of Finance for the supervision of the gambling sector.

917. The Slovak authorities should satisfy themselves that there are adequate resources allocated to set up and maintain the AML/CFT system on the policy level and that policy makers are appropriately skilled and provided with relevant training.

918. More training on TF related issues including the issues related to the implementation of SR III requirements should be provided for the NBS staff involved in the AML/CFT supervision.

919. Authorities should provide the FIU with additional resources to allow more detailed co-ordination on the national level.

920. An effective AML/CFT supervisory regime in accordance with R.30 should be established for the supervision of NPOs

921. Slovak authorities should establish an appropriate mechanism with adequate resources for the monitoring of implementation of SR III requirements.

Recommendation 32

922. More detailed and comprehensive statistics should be maintained with regard to the investigation and prosecution of ML and TF, as well as on the provisional measures applied and confiscation of proceeds of all predicate offences. All these statistics should be analysed on a regular basis to determine areas where more resources are required and to assess the effectiveness of the system.

923. Section 27 of the new AML/CFT Act should be amended to authorise the FIU to keep statistics on TF offences.

924. Slovak authorities should maintain comprehensive statistics on international co-operation and requests for assistance form foreign supervisory authorities.

925. The MoF should maintain detailed and comprehensive statistics as to the on-site examinations conducted to the gambling sector and sanctions applied.

	Rating	Summary of factors underlying rating
R.30	**PC**	• Inadequate number of staff in the FIU for dealing with its all responsibilities such as supervision and more detailed national co-ordination. • Number of staff in the Ministry of Finance for the supervision of the gambling sector is not adequate. • Not enough training focusing on or comprising the subject of TF for the NBS staff involved in the AML/CFT supervision.. • No effective mechanism exists for supervision of NPOs and supervision of the implementation of SR III requirements.
R.32	**PC**	• Inconsistencies between the various tables, even as provided most recently (following frequent contradictory updates from different authorities), lead to serious concerns with regard to the accuracy of these statistics. • Statistics collected by the FIU does not focus sufficiently on ML and TF cases, but rather on general criminality. • No statistics on international co-operation and requests for assistance form 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 are 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 are kept.

7.2 Other Relevant AML/CFT Measures or Issues

926. .N/A

7.3 General Framework for AML/CFT System

927. N/A

IV. TABLES

8 TABLE 1. RATINGS OF COMPLIANCE WITH FATF RECOMMENDATIONS

The rating of compliance vis-à-vis the FATF 40+ 9 Recommendations is made according to the four levels of compliance mentioned in the AML/CFT assessment Methodology 2004 (Compliant (C), Largely Compliant (LC), Partially Compliant (PC), Non-Compliant (NC)), or could, in exceptional cases, be marked as not applicable (N/A).

The following table sets out the ratings of Compliance with FATF Recommendations which apply to Slovakia. *It includes ratings for FATF Recommendations from the 3rd round evaluation report that were not considered during the 4th assessment visit. These ratings are set out in italics and shaded.*

Forty Recommendations	Rating	Summary of factors underlying rating[18]
Legal systems		
1. Money laundering offence	**PC**	• The definition of "property" is not sufficiently clear and the ML offence does not clearly extend to the indirect proceeds of crime. • Not all designated categories of offences are fully covered as predicates, as there is no full criminalisation of financing of individual terrorists' day-to-day activities or of the financing of the acts defined in the treaties annexed to the UN TF Convention. • There is insufficient evidence of effective implementation.
2. Money laundering offence Mental element and corporate liability	**C**	
3. Confiscation and provisional measures	**PC**	• Confiscation of indirect proceeds for ML offences is unclear. • Though the confiscation from third parties is clearly provided by the law, the relevant provisions are not used in a sufficient manner in practice. • There are not sufficient provisions for protection of the rights of bona fide third parties. • There is no clear authority to take steps to prevent or void actions, whether contractual or otherwise,

[18] These factors are only required to be set out when the rating is less than Compliant.

		where the persons involved knew or should have known that as a result of those actions the authorities would be prejudiced in their ability to recover property subject to confiscation. • Serious concerns over effectiveness of implementation.
Preventive measures		
4. Secrecy laws consistent with the Recommendations	**C**	
5. Customer due diligence	**LC**	• Lack of specific guidelines for each financial sector apart from the banking sector for improving general performance of CDD measures. • Lack of sufficiently comprehensive provision regarding reasonable measures to be taken by financial institutions in order to verify the identity of the beneficial owner. • Certain categories of low risk business can be exempted from CDD instead of requiring simplified or reduced measures. • Lack of awareness in some sectors such as securities, pension funds and payment services about the AML/CFT risks.
6. Politically exposed persons	**PC**	• No provision to verify if the beneficial owner is PEP in the Slovak Law is present. • Provisions do not apply to foreign PEPs residing in Slovakia. • The definition of PEPs is not sufficiently broad to include all categories of senior government officials. • No provision for senior management approval to continue business relationship where the customer subsequently is found to be or becomes PEP.
7. Correspondent banking	**LC**	• No enforceable requirement to document the respective AML/CFT responsibilities of each institution. • Special measures apply only to non-EU correspondent relationships.
8. New technologies and non face-to-face business	**PC**	• Effective compliance is not demonstrated. • Lack of guidance concerning new technologies

		risks and on how CDD measures should operate in non- face to face transactions.
9. Third parties and introducers	*Largely Compliant*	• *Though intermediaries are rarely used, there is the possibility for investment service providers (which are a small part of the financial sector), to act in this way and the examiners had insufficient information on their compliance.*
10. Record keeping	**LC**	• Record keeping obligation does not clearly require the maintenance of "account files and business correspondence".
11. Unusual transactions	**LC**	• No enforceable keeping term for written findings on unusual transactions exists.
12. DNFBPs – R.5, 6, 8-11	**PC**	• The same formal shortcomings under R.5, 6, 8, 10 and 11 equally apply to DNFBPs. • The awareness of the legal obligations under the AML/CFT Act especially under R.5, 6, 8 and 11 is insufficient. • The said obligations are not at all being used by most of the DNFBP in practice. • The outreach to this sector is insufficient. • The threshold of €2000 does not apply regardless whether the transaction is carried out in a single operation or in several linked operations. Recommendation 5 • The real estate agents, lawyers, notaries and other independent legal professionals and accountants have insufficient knowledge of any CDD requirements. Recommendation 6 • Insufficient level of awareness of the obligation imposed on the DNFBPs sector when it comes to dealing with PEPs Recommendations 8 and 9 • The real estate agents, lawyers, notaries and other independent legal professionals and accountants have no knowledge of any CDD requirements whatsoever. Recommendation 10 • The provisions of AML/CFT Act on record-keeping are generally not recognised, and the extent of data kept by the obliged institutions from this sector is dictated rather by the legal provisions applying directly their ore activities, than by the provisions of the AML/CFT Act on this.

		Recommendation 11 • The knowledge of obligations of unusual transactions reporting and sector specific indicators is not sufficient enough.
13. Suspicious transaction reporting	**PC**	• No clear reporting obligation 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 have an impact on the reporting of suspicious transactions. • Specific guidance or indicators for recognising suspicious transactions needed for all reporting institutions. • Effectiveness issues due to the fact that only banking and in some extent insurance sectors are reporting satisfactorily.
14. Protection and no tipping-off	*Largely Compliant*	• *It should be clarified that all civil and criminal liability is covered.*
15. Internal controls, compliance and audit	**PC**	• Lack of provision concerning timely access of the compliance officer to CDD and other relevant information • Lack of provision for compliance officers to be designated at managerial level. • No legal obligation introduced -in law, regulation or other enforceable means- for financial institutions to put in place comprehensive screening procedures to ensure high standards when hiring employees.
16. DNFBPs – R.13-15 & 21	**PC**	• The same formal shortcomings under R.13, 15 and 21 equally apply to DNFBPs. Applying Recommendation 13 • Serious lack of proper understanding of the reporting requirements among DNFBPs. • No indicators or guidelines provided to DNFBPs. • Serious concerns about the effectiveness of implementation in all aspects of Recommendation 16. • The same shortcomings as identified under R. 13 – 15, 21 and SR IV in respect of financial institutions apply to DNFBPs. Applying Recommendation 15

		• The Act on Gambling does have certain provisions related to employees and shareholder screening. However, there are no such provisions for other DNFBPs. • The poor recognition of the obligation imposed by the AML/CFT Act (especially those on CDD measures) hampers the overall effectiveness of the execution of training obligation. • Lack of an explicit obligation for DNFBPs to have internal controls or to appoint a compliance officer at the managerial level. • There is no explicit obligation to have internal controls by the DNFBP, nor a compliance officer at managerial level. • No independent audit function is required. • The trainings provided to this sector are not effective as the recognition of the obligations under the AML/CFT Act remains poor. Applying Recommendation 21 • As the obligations arising from R.21 are not met in regard to financial institutions in general, they also do not apply to DNFBP.
17. Sanctions	**PC**	• Sanctions are mostly not applicable to directors and senior management by the FIU and MoF. • Full range of sanctions is not available for the use of the FIU. • No provisions available to avoid double sanctioning.
18. Shell banks	*Largely compliant*	• *The Act on Banks imposes licensing conditions which require conditions for establishment of banks with a physical presence in Slovakia. Decree No. 9/2004 of the NBS establishes the particulars to be required of an applicant for a banking license. Both sets of provisions could act as a barrier against shell banks operating in Slovakia. However, there is no legally binding prohibition on financial institutions on entering into or continuing correspondent banking relationships with shell banks. Neither is there any obligation on financial institutions to satisfy themselves that a respondent financial institution in a foreign country does not permit its accounts to be used by shell banks.*
19. Other forms of reporting	**C**	
20. Other DNFBPs and secure transaction techniques	**LC**	• No national overreaching strategy on the development and use of modern secure techniques.

21. Special attention for higher risk countries	**NC**	• No enforceable requirement for financial institutions to pay special attention to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations. • No effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other countries. • No mechanisms in place that would enable the authorities to apply counter-measures to countries that do not apply or insufficiently apply FATF recommendations. • No requirement to examine, as far as possible, the background and purpose when transactions have no apparent economic or visible lawful purpose, and to make available written findings to assist competent authorities and auditors.
22. Foreign branches and subsidiaries	**LC**	• No requirement to ensure that foreign branches and subsidiaries observe AML/CFT measures consistent with the FATF Recommendations other than the requirements of R. 5 and 10. • No requirement to apply the higher standard where requirements differ. • The requirement to ensure observing AML/CFT measures in respect of branches and subsidiaries is limited to institutions located in non-EU Member States (third countries).
23. Regulation, supervision and monitoring	**LC**	• The level of on-site inspections conducted by the MoF is not sufficient enough.
24. DNFBPs - Regulation, supervision and monitoring	**PC**	• No clear strategy for DNFBP supervision demonstrated to the evaluators. • Not sufficient outreach to this sector, also in the way of on-site inspections. • Effectiveness concerns about the supervision of DNFBPs by the FIU.
25. Guidelines and Feedback	**PC**	• The co-operation with the DNFBP is unsatisfactory. (25.2) • Not all reporting entities have received specific guidelines. • No sector specific guidelines to cover financial market participants other than banks. (25.1) • Feedback provided to reporting entities not always

		substantive and descriptive enough. (25.2) • Sector specific guidelines for DNFBPs do not cover the entire sectors. • More detailed and prompt case-by-case feedback is needed.
Institutional and other measures		
26. The FIU	**PC**	• Concerns over 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 should contain information on trends and typologies. • The FIU does not concentrate sufficiently on ML and TF which should be the main focus, but rather on all criminal offences equally. • Effectiveness of the FIU work on specific ML/FT cases cannot be appropriately established since statistics relate to all criminal offences.
27. Law enforcement authorities	*Largely compliant*	• *While there are designated law enforcement authorities with responsibility for money laundering and terrorist financing investigations, with adequate powers, there is a reserve on the effectiveness of money laundering and terrorist financing investigations.*
28. Powers of competent authorities	*Compliant*	
29. Supervisors	**LC**	• Not enough focus is placed in the scope of the on-site visits on issues of SR.VII.
30. Resources, integrity and training	**PC**	• Inadequate number of staff in the FIU for dealing with its all responsibilities such as supervision and more detailed national co-ordination. • Number of staff in the Ministry of Finance for the supervision of the gambling sector is not adequate. • Not enough training focusing on or comprising the subject of TF for the NBS staff involved in the AML/CFT supervision.. • No effective mechanism exists for supervision of NPOs and supervision of the implementation of SR III requirements.

31. National co-operation	**PC**	• Lack of sufficient co-ordination between major players of the AML/CFT regime. • More effective mechanisms needed to co-ordinate at the operational level. • More detailed statistics are required across the board to assist proper co-ordinated policy analysis. • The mechanisms in place not utilised effectively.
32. Statistics	**PC**	• Inconsistencies between the various tables, even as provided most recently (following frequent contradictory updates from different authorities), lead to serious concerns with regard to the accuracy of these statistics. • Statistics collected by the FIU does not focus sufficiently on ML and TF cases, but rather on general criminality. • 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 are 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 are kept.
33. Legal persons – beneficial owners	**PC**	• Lack of adequate transparency concerning beneficial ownership and control of legal persons. • Access to information on beneficial ownership and control of legal persons, when there is such access, is not always timely. • No measures to ensure the adequacy, accuracy and currency of the beneficial ownership information. • Transparency of bearer shares.
34. Legal arrangements – beneficial owners	*N/A*	
International Co-operation		
35. Conventions	**PC**	• Reservations about certain aspects of the implementation of the Vienna, Palermo and the TF

		Conventions. • Effectiveness of the implementing the standards in relation to ML and TF gives rise to doubts. • Financing of some of the Acts defined in the treaties appearing in the Annex to the Convention are not criminalised as terrorist financing offence.
36. Mutual legal assistance (MLA)	**LC**	• Lack of criminalisation of individual terrorists' for purposes other than specific acts of terrorism could negatively impact mutual legal assistance based on dual criminality. • No information was provided on whether the authorities have considered best venue for prosecution in cases subject to prosecution in more than one country, other than as provided under the membership in Eurojust.
37. Dual criminality	**LC**	• The limitations in the definition of the financing of terrorism may limit the ability of the Slovak Republic to provide MLA.
38. MLA on confiscation and freezing	**PC**	• The limitations in the definition of the financing of terrorism may limit the ability of the Slovak Republic to provide MLA. • Difficulties in forfeiting property from third parties may limit the ability of the Slovak Republic to provide MLA. • No evidence of concrete arrangements for co-ordination of seizure and confiscation actions with other countries or for sharing confiscated assets with them, other than those provided under the Framework Decision applicable for EU Member States. • Absence of adequately detailed statistics makes judgment on effectiveness difficult.
39. Extradition	*Largely Compliant*	• *In the absence of statistics it is not possible to determine whether these requests are handled without undue delay.*
40. Other forms of co-operation	**LC**	• Lack of detailed statistics undermines the assessment of effectiveness. (for supervisory authorities)
Nine Special Recommendations		
SR.I Implement UN instruments	**PC**	• Financing of some of the Acts defined in the treaties appearing in the Annex to the Convention

		are not criminalised. • Implementation of UNSCRs 1267 and 1373 is not yet sufficient.
SR.II Criminalise terrorist financing	**PC**	• No full criminalisation of financing of an individual terrorist's day-to-day activities. • Non-criminalisation of the financing of the acts defined in the treaties annexed to the TF Convention. • Effectiveness concerns.
SR.III Freeze and confiscate terrorist assets	**PC**	• The situation envisaged by the UNSCR 1267 for the freezing of assets in the event of control or possession of assets by persons acting in the name of or at the direction of designated persons or entities is not covered in Council Regulation No. 881/2002. • The time taken for EU Regulations to be adopted aimed at dealing with amendments made to the list published by the 1267 Committee can be relatively long; in this respect the obligation to freeze terrorist funds without delay is not observed. • 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. • Insufficient monitoring for compliance of financial institutions and DNFBPs..
SR.IV Suspicious transaction reporting	**PC**	• No clear reporting obligation 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 limit the reporting obligation. • Indicators or guidelines to reporting entities limited to cases related to international sanctions. No specific indicators provided except two, presented in the AML/CFT Act and one another published on the FIU website. • Only banks reported UTRs regarding TF (effectiveness issues).

SR.V International co-operation	**LC**	• The limitations in the definition of the financing of terrorism may limit the ability of the Slovak Republic to provide MLA. • Lack of detailed statistics undermines the assessment of effectiveness.
SR.VI AML requirements for money/value transfer services	*Largely Compliant*	• *The NBS is obliged to register and license the persons performing money or value transfer services. However there was no provision determining what kind of information regarding transactions should be recorded as a minimum, no regulation requiring money exchange companies to examine the purpose of complex, unusual large transactions or unusual patterns of transactions.*
SR.VII Wire transfer rules	**C**	
SR.VIII Non-profit organisations	**NC**	• No risk assessment of NPOs has been undertaken, although there is some transparency and annual reporting structure for foundations. • No review of the adequacy of legislation to prevent the abuse of NPOs for TF has been undertaken. • Authorities do not conduct outreach or provide guidance on TF to the NPO sector. • There is no supervision or monitoring of the NPO sector as envisaged by the Interpretative Note to SR VIII. • No obligation for keeping detailed domestic and international transaction records. • 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.
SR.IX Cross Border declaration and disclosure	**PC**	• Inconsistency regarding reporting forms exist in the legal framework due to the existence of two pieces of legislation dealing with the cash reporting system (one on the EU level and one national). • The system itself is rather ineffective since there are a very low number of declared transfers, no cases of false declaration or failure to declare, no cases of ML or TF triggered by the system and no sanctions imposed for false declaration. • Deficiencies in the implementation of SR III may have an impact on the effectiveness of the regime.

9 TABLE 2: RECOMMENDED ACTION PLAN TO IMPROVE THE AML/CFT SYSTEM

AML/CFT System	Recommended Action (listed in order of priority)
1. General	
2. Legal System and Related Institutional Measures	
2.1 Criminalisation of Money Laundering (R.1 & 2)	• Slovak authorities should define "property" in accordance with the FATF Methodology. • Slovak authorities should analyse the reasons for the apparent discrepancy between the extent of the organised crime in Slovakia and the quality of ML cases brought forward and which have resulted in convictions. They should further assess the reasons of the ineffective use of ML investigation and prosecution as a tool to combat organised crime and major proceeds generating offences. In the light of these assessments Slovak authorities should take appropriate steps including awareness raising activities for the police, prosecutors and judges.
2.2 Criminalisation of Terrorist Financing (SR.II)	• The financing of individual terrorist's day-to-day activities should be criminalised as required by criterion II.1. • The SCC should be revised to ensure proper criminalisation of financing of the acts arising from the Convention by amending Section 419 (b) so that it covers financing of offences under the other sections of the SCC criminalising the acts pursuant to the treaties listed in the annexes to the UN TF Convention.
2.3 Confiscation, freezing and seizing of proceeds of crime (R.3)	• Though Slovakia has taken some legislative steps to comply with R.3, further legislative steps in order to fully comply with international standards appear to be needed. • Effectiveness of the implementation of seizure/freezing measures and forfeiture/confiscation should be improved as a matter of priority. • Precise statistics on amounts frozen, seized, forfeited and confiscated related to ML, TF and criminal proceeds should be maintained so as to be able to establish an overview of the effectiveness of the system. • Authority should be given to allow for confiscation from third parties and to prevent or void actions, where the persons involved knew or should have known that as a

	result of those actions the authorities would be prejudiced in the ability to recover property subject to confiscation.
2.4 Freezing of funds used for terrorist financing (SR.III)	• The Slovak Republic needs to develop guidance and communication mechanisms with all financial institutions and DNFBPs and a clear and publicly known procedure for de-listing and unfreezing in appropriate cases in a timely manner. • A more robust and effective mechanism, beyond the periodic reports submitted by the banking sector, for the monitoring of the compliance of reporting entities with the SR III requirements should be established. • The Slovak authorities should take legislative or other appropriate steps to create a fully compliant freezing system as required under SR III.
2.5 The Financial Intelligence Unit and its functions (R.26)	• The Slovak authorities should introduce formal safeguards to ensure the FIU's operational independence and autonomy. • The FIU's position in the police structure and in the AML/CFT system as a whole should be revisited. • The FIU should be encouraged to concentrate more on ML and TF cases. • The FIU should continue with its activities in publication of periodic reports and these reports should include information on trends and typologies.
2.6 Cross Border Declaration & Disclosure (SR IX)	• The Slovak authorities should remove all inconsistencies that exist in the legal framework so as to avoid legal uncertainty with regard to the implementation of SRIX. • The Slovak authorities should take steps to raise awareness of arriving and departing travellers by making the sign alerting travellers to the requirements at ports of entry and exit much more visible, and perhaps in several languages. • Specialised training activities related to SR.IX for the staff of the customs administration should be established. • The Slovak authorities should take steps to heighten the awareness of customs officers and all others competent bodies present at borders (e.g. police, immigration office) of the obligations arising from SR IX. • Clear and effective mechanisms and procedures should be developed for daily operational co-operation and co-ordination in exchange of intelligence and other information between all bodies present at borders.
3. Preventive Measures – Financial Institutions	

3.1 Risk of money laundering or terrorist financing	• A formal risk assessment should be undertaken to assess the areas of vulnerability to money laundering and terrorist financing in Slovakia.
3.2 Customer due diligence, including enhanced or reduced measures (R.5 to 8)	• Slovak authorities should introduce a more comprehensive provision regarding reasonable measures to be taken by financial institutions in order to verify the identity of the beneficial owner. • Slovak authorities should review the identification process in respect of low risk customers/circumstances/businesses to one of reduced or simplified customer due diligence instead of granting exemptions. • Slovak authorities should issue guidance for some sectors such as securities, pension funds and payment services to make them aware of sectoral AML/CFT risks. • The Slovak authorities are encouraged to review the definition of PEP to fully reflect the one provided in the Glossary to the FATF Recommendations. Especially it should cover senior politicians, senior government officials (for example non-political heads of ministries) and important party officials. • Although the AML/CFT Act obliges to undertake enhanced due diligence measures when establishing a business relationship with a PEP, there is no specific requirement to find out whether the beneficial owner of the contracting party might be a PEP. The Slovak authorities should consider addressing this issue either in law or regulation or other enforceable means. • As the FATF standard should be applicable to persons entrusted with prominent public functions in a foreign country, it is advisable not to limit the provisions of Slovak law only to foreign PEPs residing abroad. • The Slovak authorities should introduce an obligation by law, regulation or other enforceable means for obtaining senior management approval to continue business relationship where the customer subsequently is found to be or becomes a PEP. • Slovak authorities should consider providing in law, regulation or other enforceable means an obligation for financial institutions to document the respective AML/CFT responsibilities of each institution on the cross-border correspondent banking relationship, for both EU and non-EU correspondent relationship. • Slovak authorities should extend the enhanced CDD measures to respondent banks within the EU. • Specific guidance regarding new technological risks and the need for internal policies within financial institutions

	to prevent the misuse of technological developments in money laundering or financing of terrorism need to be issued.
3.3 Financial institution secrecy or confidentiality (R.4)	
3.4 Record keeping and wire transfer rules (R.10 & SR.VII)	• Though different sectoral laws appears to have provisions and authorities see no problem in practice, a clear obligation should be placed upon financial institutions in the AML/CFT Act with a view to ensuring that transaction records to be kept are sufficient as required under essential criterion 10.1.1. • Section 19 of the AML/CFT should be amended to explicitly require keeping of account files and business correspondence for at least five years following the termination of an account or business relationship.
3.5. Monitoring of transactions and relationship reporting (R.11 & R.21)	• A keeping term for written findings should be determined by law, regulation or other enforceable means with a view to ensuring that financial institutions keep available such findings for at least five years. • There should be effective measures in place to ensure that financial institutions are advised of concerns about weakness in the AML/CFT systems of other countries. • The Slovak legal framework should include a general provision concerning the obligation of financial institutions to pay special attention to business relationships and transactions with persons from or in countries that fail or insufficiently apply FATF Recommendations. • In particular, the Slovak AML/CFT legal framework should include a provision concerning the obligation for entities to examine as far as possible those transactions that have no apparent economic or visible lawful purpose and to make written findings available to assist competent authorities (e.g. supervisors, law enforcement agencies and the FIU) and auditors. • The Slovak authorities should be legally empowered to apply counter-measures within the meaning of Recommendation 21.
3.6 Suspicious transaction reports and other reporting (R.13, 19, 25 & SR.IV)	• Indicators for recognising suspicious transactions as guidelines for other financial sectors (securities market, currency exchange etc) are needed and should be issued by the FIU and other competent bodies. • Not all designated categories of offences are fully covered as predicates, as incrimination of the financing of an individual terrorist is not covered. The Slovak authorities should take legislative measures in order to

	ensure that there is a clear obligation to report to the FIU when an obliged entity suspects or has reasonable grounds to suspect that funds are linked or related to, or to be used for terrorism, terrorist acts or by terrorist organisations or those who finance terrorism. • Authorities should take measures to provide the financial sector with a comprehensive set of guidelines for recognising suspicious transactions that are related to TF. • More guidelines to financial sector should be provided to financial sector in order to improve the reporting regime. • Authorities should focus more on the issue of providing guidelines due to the fact that not all the sectors have received specific guidance and that the guidelines already issued, except for the banking sector, are very brief and in most of the cases relate to very specific cases that the FIU experienced in its work, thus having limited space to be used. • Notwithstanding the progress achieved in relation to case-by-case feedback, particularly as financial institutions receive tables on every UTR quarterly, the Slovak authorities are encouraged to continue with their efforts in this field and to include more substantial and descriptive information in the tables that are already disseminated to reporting entities. • More focus should be placed on improving the co-operation with the DNFBP sector in the respect of feedback on STRs. Though the financial institutions are generally satisfied with the feedback they receive, the evaluators recommend that prompt and more detailed feedback should be provided in order to improve the effectiveness of implementing Recommendation 25.
3.7 Internal controls, compliance, audit and foreign branches (R.15 & 22)	• The Slovak legal framework does not contain a provision concerning timely access of the compliance officer to customer identification data and other CDD information, transaction records and other relevant information, though this deficiency is partly addressed by the NBS Methodological guidance and the overall approach of the financial institutions. It is, however, advisable to clearly state such provision in the law, to ensure full compliance with R.15. • The Slovak authorities should clearly state in law, regulation or other enforceable means that the compliance officer should be appointed at a managerial level. • The Slovak authorities should introduce a legal obligation in law, regulation or other enforceable means for financial institutions to put in place comprehensive screening procedures to ensure high standards when

	hiring employees. • It is recommended to extend the requirements in Section 24 to the FATF Recommendations in general, and not only to Recommendations 5 and 10. • A requirement should be introduced to ensure observing AML/CFT measures in respect of branches and subsidiaries of the institution located in EU Member or European Economic Area. • A requirement should be introduced to the effect that where the minimum AML/CFT requirements of the home and host countries differ, branches and subsidiaries in host countries should be required to apply the higher standard, to the extent that local (i.e. host country) laws and regulations permit.
3.8 The supervisory and oversight system - competent authorities and SROs. Role, functions, duties and powers (including sanctions) (R.23, 29, 17 & 25)	• There should be more training for the NBS staff focusing on or comprising the subject of TF. • It should be further elaborated by the NBS whether the on-site inspections procedure should also include a detailed description of supervisory measures to be taken during an on-site visit by the NBS staff, as the lack of those provisions may be deemed a contingency lowering the effectiveness of the performed on-site visits. • Slovak authorities should take necessary steps with a view to ensuring the FIU to use a wide and dissuasive range of sanctions provided in the special laws. • The Slovak authorities are advised to consider whether the detailed provisions on avoiding double sanctioning should be clearly stated in the MoU between the NBS and the FIU. • It is recommended that the FIU and the MoF should exchange inspection plans to increase the effectiveness of actions undertaken by each of the authority. • Although the range of sanctions available is broadly inline with criterion 17.4, it may not be used by the FIU, which in effect leads to a conclusion that directors and senior management of financial institutions cannot be sanctioned for AML/CFT Act's violations. This issue should be clearly addressed by the Slovak authorities. • The Slovak authorities should issue guidelines to financial market participants other than banks, and the FX offices as well. • The NBS as the supervisor has enough and adequate powers to deal with its responsibilities. The NBS on-site visits are thorough and deal generally with all important parts of the financial institutions AML/CFT regime, notwithstanding the deficiencies in the procedure stated above. There is, however, a need to place more emphasis

	on verifying the compliance with SR.VII during on-site visits. • It is unclear how thorough and in depth are the on-site inspections conducted by the MoF in gambling operators. Otherwise it seems the MoF is properly equipped with the legal duties and powers to deal with the tasks assigned to them in the AML/CFT regime of Slovakia. More emphasis should, however, be placed on the proper number of employees to deal with the supervisions. • Though the range of sanctions (already discussed in this report) which can be imposed on the institutions and over their directors and senior managers is broad enough, the FIU and the MoF should be empowered to impose sanctions on physical persons.
4. Preventive Measures – Non-Financial Businesses and Professions	
4.1 Customer due diligence and record-keeping (R.12)	• There is an urgent need for an extensive outreach to the DNFBP sector to make them aware of AML/CFT issues and their obligation under the AML/CFT Act, and Recommendation 5, 6, 8, 10 and 11. • Actions should be taken with immediate effect to make the real estate agents, lawyers, notaries and other independent legal professionals and accountants fully aware of their obligations under the AML/CFT Act, and to apply them in practice. • It is of great concern that the obligation regarding PEPs are not at all complied with by this sector. This must be addressed by the Slovak authorities, mainly by providing more extensive outreach to this sector.
4.2 Suspicious transaction reporting (R.16)	• The authorities should tailor and implement more comprehensive outreach and training programme targeted to DNFBP to enhance the awareness and knowledge of the UTR detection and reporting. • Guidelines and indicators for recognising suspicious transactions similar to those given to the banking sector in the Methodological guidance should be issued for DNFBP as well. • The Slovak authorities should consider the way to meet the R.15 standards to DNFBPs in the field of appointing the compliance officer and maintaining independent audit function. • The poor outreach to this sector, not satisfactory effectiveness of the trainings and an insufficient number of on-site inspections should be addressed by the Slovak authorities, preferably in a manner of an ongoing process.

	• There should be provisions related to employees and shareholders screening, which at this point only apply to gambling operators and other institutions that fall under the jurisdiction of the Gambling Act. • When the legal framework will be improved by the Slovak authorities it also should be applicable to the DNFBP. The awareness raising programs for the implementation of Recommendation 21 should be also considered.
4.3 Regulation, supervision and monitoring (R.24-25)	• The resources of the FIU needs to be increased to fully embrace the supervision requirements over DNFBP sector, as the resources now present can only be deem sufficient as far as the supervision over financial sector goes. • There is an urgent need for sector specific guidelines on AML/CFT issues to DNFBPs other than those already covered by the FIU.
4.4 Other non-financial business and professions/ Modern secure transaction techniques (R.20)	• The Slovak authorities are encouraged to develop measures to encourage the development and use of modern and secure techniques for financial transactions that are less vulnerable to ML.
5. Legal Persons and Arrangements & Non-Profit Organisations	
5.1 Legal persons – Access to beneficial ownership and control information (R.33)	• Slovakia is recommended to review its commercial, corporate and other laws with a view to provide transparency with respect to beneficial ownership.
5.2 Non-profit organisations (SR.VIII)	• The Slovak authorities should review the risks of terrorist financing in the NPO sector, as well as the current system of laws and regulation in this field so as to adequately address the risks that this sector presents. • The authorities should improve the supervision over the NPOs to ensure that all types of NPOs are under appropriate supervision with regard to the risks of financing of terrorism. • Awareness raising measures need to be adopted relating to the NPO sector on the risk of terrorist abuse and available measures to protect the sector against such abuse.
6. National and International Co-operation	
6.1 National co-operation and co-ordination (R.31)	• The Slovak authorities should consider taking steps to strengthen the IIGE perhaps on a more senior level. • As more effective mechanisms are needed at operational

	level, Slovak authorities should consider creating joint investigative teams or other forms of interagency co-ordination mechanisms, perhaps lead by prosecutors, in order to investigate and bring before the courts more ML cases which are related to major proceed-generating criminal offences. • Strategic co-ordination and collective review of the performance of the system as a whole (including analysis, where appropriate, of better statistical information) needs developing in more detail. More detailed statistics are required across the board to assist proper strategic analysis.
6.2 The Conventions and UN Special Resolutions (R.35 & SR.I)	• Slovakia is urged to amend its SCC to fully cover ML and TF offences and thus fully implement the Vienna, Palermo and the UN TF Conventions. • Measures still need to be taken in order to properly implement UNSCRs 1267 and 1373.
6.3 Mutual Legal Assistance (R.36 - 38 & SR.V)	• The limitations in the definition of financing of terrorism should be removed.
6.5 Other Forms of Co-operation (R.40 & SR.V)	• Due to the lack of detailed statistics it was not possible to assess how effectively the Slovak authorities were responding to international co-operation requests and therefore, it is recommended that procedures are put in place to centrally record and monitor all international co-operation requests on matters related to ML and TF. • It is advisable for the NBS to keep detailed statistics on their international co-operation, as there are non whatsoever. • The Slovak authorities should consider the feasibility of international exchange of information in respect of gambling supervision conducted by the MoF.
7. Other Issues	
7.1 Resources and statistics (R. 30 & 32)	• The Slovak authorities could give more specific training on ML and TF offences, and the seizure, freezing and confiscation of property that is the proceeds of crime or is to be used to finance terrorism to police, prosecutors and judges. • More resources and staff should be dedicated to the FIU for its activities in the supervision field and for its performance of a more effective national co-ordination role. • More staff and resources should be provided to the Ministry of Finance for the supervision of the gambling sector.

	• The Slovak authorities should satisfy themselves that there are adequate resources allocated to set up and maintain the AML/CFT system on the policy level and that policy makers are appropriately skilled and provided with relevant training. • More training on TF related issues including the issues related to the implementation of SR III requirements should be provided for the NBS staff involved in the AML/CFT supervision. • Authorities should provide the FIU with additional resources to allow more detailed co-ordination on the national level. • An effective AML/CFT supervisory regime in accordance with R.30 should be established for the supervision of NPOs • The Slovak authorities should establish an appropriate mechanism with adequate resources for the monitoring of implementation of SR III requirements. • More detailed and comprehensive statistics should be maintained with regard to the investigation and prosecution of ML and TF, as well as on the provisional measures applied and confiscation of proceeds of all predicate offences. All these statistics should be analysed on a regular basis to determine areas where more resources are required and to assess the effectiveness of the system. • Section 27 of the new AML/CFT Act should be amended to authorise the FIU to keep statistics on TF offences. • The Slovak authorities should maintain comprehensive statistics on international co-operation and requests for assistance form foreign supervisory authorities. • The MoF should maintain detailed and comprehensive statistics as to the on-site examinations conducted to the gambling sector and sanctions applied.

10 TABLE 3: AUTHORITIES' RESPONSE TO THE EVALUATION (IF NECESSARY)

RELEVANT SECTIONS AND PARAGRAPHS	COUNTRY COMMENTS

V. COMPLIANCE WITH THE 3RD EU AML/CFT DIRECTIVE

Slovakia is a member country of the European Union since 2004. It has implemented **Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing** (hereinafter: "the Directive") and the **Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis**.

The following sections describe the major differences between the Directive and the relevant FATF 40 Recommendations plus 9 Special Recommendations.

1.	**Corporate Liability**
Art. 39 of the Directive	Member States shall ensure that natural and legal persons covered by the Directive can be held liable for infringements of the national provisions adopted pursuant to this Directive.
FATF R. 2 and 17	Criminal liability for money laundering should extend to legal persons. Where that is not possible (i.e. due to fundamental principles of domestic law), civil or administrative liability should apply.
Key elements	The Directive provides no exception for corporate liability and extends it beyond the ML offence even to infringements which are based on national provisions adopted pursuant to the Directive. What is the position in your jurisdiction?
Description and Analysis	With the enactment of the Act no. 224/2010 Coll. amending the Criminal Code, Slovakia has introduced criminal liability for legal persons to the Slovak legal system. The amendments that came into force on the 1st September 2010 have made it possible to impose protective/security measures on legal entities and confiscation of a property belonging to a legal entity. Sections 83a and 83b of the SCC (See Annex V) now enable the courts to impose monetary sanctions if the criminal offence is committed under certain circumstances, while the court considers, *inter alia*, the seriousness of the committed criminal offence and additional elements as specified in Sections 83a & 83b of the SCC. However, it should be noted that according to Section 83a, the court might impose the confiscation of a sum of money in an amount of €800– €1,660,000. Sections 83a & 83b of the SCC could be regarded as criminal liability as it is regulated in the SCC, applied in criminal proceedings by the Courts by taking into account the seriousness of the criminal offence, circumstances of the commission of the criminal offence and consequences for the legal person. In terms of sanctions, the court shall confiscate property of a legal person if the conditions listed in paragraph 1 of Section 83b of the SCC are fulfilled, i.e. that the property or part thereof were obtained by a crime or as proceeds of a crime related to exercising the right to represent, make decisions in the name of, or carry out the control within, the legal person or related to negligence concerning the supervision or due diligence

	within that legal person. If the court does not impose the confiscation of the property, it is obliged to impose the confiscation of a sum of money (€800 – 1 660 000), considering the seriousness of the offence, its extent, the benefit gained, the damage caused, the circumstances of the commission, and the consequences of the confiscation for the legal person.
Conclusion	This issue is covered.
Recommendations and Comments	N/A

2.	**Anonymous accounts**
Art. 6 of the Directive	Member States shall prohibit their credit and financial institutions from keeping anonymous accounts or anonymous passbooks.
FATF R. 5	Financial institutions should not keep anonymous accounts or accounts in obviously fictitious names.
Key elements	Both prohibit anonymous accounts but allow numbered accounts. The Directive allows accounts or passbooks on fictitious names but always subject to full CDD measures. What is the position in your jurisdiction regarding passbooks or accounts on fictitious names?
Description and Analysis	The Slovak Law (Section 24 para 2 of the AML/CFT Act and Art. 89 para 1 of the Act on Banks) clearly prohibits starting any business relationship without the proper identification of a client, therefore prohibiting from opening any sort of anonymous products. It can also be derived from the Act that any person now wishing to withdraw founds from any anonymous product existing, would have to be identified. Since 1 September 2001, the opening of new bearer passbooks is prohibited (according to the Slovak Civil Code). Concerning the pay outs of bearer deposits regime, until the end of 2011 a passbook holder has the right to be paid out. Until 2011, the Ministry of Finance paid out a bearer of a passbook or a bearer of other bearer securities on the condition that the identification is done. The AML/CFT Act obliges financial institutions to perform identification of a customer and verification of his identity. However, there is no explicit prohibition of anonymous accounts or accounts in fictitious names.
Conclusion	In Slovak Law there is no explicit prohibition of anonymous accounts or accounts in fictitious names
Recommendations and Comments	The Slovak authorities may wish to consider addressing the said issue.

3.	**Threshold (CDD)**
Art. 7 b) of the Directive	The institutions and persons covered by the Directive shall apply CDD measures when carrying out occasional transactions amounting to €15 000 or more.
FATF R. 5	Financial institutions should undertake CDD measures when carrying out occasional transactions above the applicable designated threshold.
Key elements	Are transactions and linked transactions of €15 000 covered?
Description and Analysis	According to Section 10 paragraph 2 letter b) of the AML/CFT Act CDD shall be performed when carrying out an occasional transaction outside a business relationship worth at least €15,000 regardless of whether the transaction is carried out in a single operation or in several linked operations which are or may be connected
Conclusion	Transactions and linked transactions of €15,000 are covered
Recommendations and	N/A

Comments	

4.	**Beneficial Owner**
Art. 3(6) of the Directive (see Annex)	The definition of 'Beneficial Owner' establishes minimum criteria (percentage shareholding) where a natural person is to be considered as beneficial owner both in the case of legal persons and in the case of legal arrangements
FATF R. 5 (Glossary)	'Beneficial Owner' refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or legal arrangement.
Key elements	Which approach does your country follow in its definition of "beneficial owner"? Please specify whether the criteria in the EU definition of "beneficial owner" are covered in your legislation.
Description and Analysis	Beneficial owner, in the Slovak Law, means a natural person for the benefit of whom a transaction is being carried out or a natural person who: 1. has a direct or indirect interest or their total at least 25 % in the equity capital or in voting rights in a customer being a legal entity - entrepreneur including bearer shares, unless that legal entity is an issuer of securities admitted to trading on a regulated market which is subject to disclosure requirements under a special regulation, 2. is entitled to appoint, otherwise constitute or recall a statutory body, majority of members of a statutory body, majority of supervisory board members or other executive body, supervisory body or auditing body of a customer being a legal entity –entrepreneur, 3. in a manner other than those referred to in subsections 1 and 2 controls a customer being a legal entity –entrepreneur, 4. is a founder, a statutory body, a member of a statutory body or other executive body, supervisory body or auditing body of a customer being a corporation or is entitled to appoint, otherwise constitute or recall those bodies, 5. is a beneficiary of at least 25% of funds supplied by a corporation, provided the future beneficiaries of those funds are designated or 6. ranks among those persons for whose benefit a corporation is established or operates, unless the future beneficiaries of funds of the corporation are designated.
Conclusion	The legal definition of the beneficial owner corresponds with the definition of the Third EU AML/CFT Directive.
Recommendations and Comments	N/A

5.	**Financial activity on occasional or very limited basis**
Art. 2 (2) of the Directive	Member States may decide that legal and natural persons who engage in a financial activity on an occasional or very limited basis and where there is little risk of money laundering or financing of terrorism occurring do not fall within the scope of Art. 3(1) or (2) of the Directive. Art. 4 of Commission Directive 2006/70/EC further defines this provision.
FATF R. concerning	When a financial activity is carried out by a person or entity on an

financial institutions	occasional or very limited basis (having regard to quantitative and absolute criteria) such that there is little risk of money laundering activity occurring, a country may decide that the application of anti-money laundering measures is not necessary, either fully or partially (2004 AML/CFT Methodology para 23; Glossary to the FATF 40 plus 9 Special Recs.).
Key elements	Does your country implement Art. 4 of Commission Directive 2006/70/EC?
Description and Analysis	Article 4 of Commission Directive 2006/70/EC was not implemented in the Slovak Republic.
Conclusion	Article 4 of Commission Directive 2006/70/EC was not implemented in the Slovak Republic.
Recommendations and Comments	N/A

6.	**Simplified Customer Due Diligence (CDD)**
Art. 11 of the Directive	By way of derogation from the relevant Article the Directive establishes instances where institutions and persons may not apply CDD measures. However the obligation to gather sufficient CDD information remains.
FATF R. 5	Although the general rule is that customers should be subject to the full range of CDD measures, there are instances where reduced or simplified measures can be applied.
Key elements	Is there any implementation and application of Art. 3 of Commission Directive 2006/70/EC which goes beyond the AML/CFT Methodology 2004 criterion 5.9?
Description and Analysis	Section 11 of the AML/CFT Act of the Slovak Republic states contingencies and conditions under which a financial institutions or any other obliged entity may perform simplified customer due diligence.
Conclusion	The said provisions are broadly in line with Article 3 of Commission Directive 2006/70/EC.
Recommendations and Comments	N/A

7.	**Politically Exposed Persons (PEPs)**
Art. 3 (8), 13 (4) of the Directive (see Annex)	The Directive defines PEPs broadly in line with FATF 40 (Art. 3(8)). It applies enhanced CDD to PEPs residing in another Member State or third country (Art. 13(4)). Directive 2006/70/EC provides a wider definition of PEPs (Art. 2) and removal of PEPs after one year of the PEP ceasing to be entrusted with prominent public functions (Art. 2(4)).
FATF R. 6 and Glossary	Definition similar to Directive but applies to individuals entrusted with prominent public functions in a foreign country.
Key elements	Does your country implement Art. 2 of Commission Directive 2006/70/EC, in particular Art. 2(4), and does it apply Art. 13(4) of the Directive?
Description and Analysis	Section 6 of the AML/CFT Act implements the definition of PEP, which is in line with the third Directive. Each time a client is identified as a PEP, enhanced due diligence measures must be undertaken. Such measures reflect those stated in Article 13 (4) of the Directive.
Conclusion	Slovakia has implemented Article 2(4) of Commission Directive

	2006/70/EC and it applies Article 13(4) of the Directive as well.
Recommendations and Comments	N/A

8.	**Correspondent banking**
Art. 13 (3) of the Directive	For correspondent banking, Art. 13(3) limits the application of Enhanced Customer Due Diligence (ECDD) to correspondent banking relationships with institutions from non-EU Member States.
FATF R. 7	Recommendation 7 includes all jurisdictions.
Key elements	Does your country apply Art. 13(3) of the Directive?
Description and Analysis	Section 11 of the AML/CFT Act allows the financial institutions to apply simplified due diligence measures to a credit or financial institution from an EU Member State or an equivalent third country. Should however such institution located in another country, enhanced CDD measures must be implemented in accordance with Section 12 of the AML/CFT Act.
Conclusion	Slovakia applies Article 13 (3) of the Third EU AML/CFT Directive.
Recommendations and Comments	N/A

9.	**Enhanced Customer Due Diligence (ECDD) and anonymity**
Art. 13 (6) of the Directive	The Directive requires ECDD in case of ML or TF threats that may arise from products or transactions that might favour anonymity.
FATF R. 8	Financial institutions should pay special attention to any money laundering threats that may arise from new or developing technologies that might favour anonymity [...].
Key elements	The scope of Art. 13(6) of the Directive is broader than that of FATF R. 8, because the Directive focuses on products or transactions regardless of the use of technology. How are these issues covered in your legislation?
Description and Analysis	According to Section 14 paragraph 2 letter b of the AML/CFT Act obliged entities shall pay special attention to "any risk of legalisation or terrorist financing that may arise from a type of transaction, a particular transaction or new technological procedures while carrying out transactions that may support anonymity and is obliged to take appropriate measures, if needed to prevent their use for the purposes of legalisation and terrorist financing"
Conclusion	The Slovak law is in line with Article 13 (6) of the Directive.
Recommendations and Comments	N/A

10.	**Third Party Reliance**
Art. 15 of the Directive	The Directive permits reliance on professional, qualified third parties from EU Member States or third countries for the performance of CDD, under certain conditions.
FATF R. 9	Allows reliance for CDD performance by third parties but does not specify particular obliged entities and professions which can qualify as third parties.
Key elements	What are the rules and procedures for reliance on third parties? Are there special conditions or categories of persons who can qualify as third parties?
Description and	Section 13 of the AML/CFT Act states that the third party may only be a

Analysis	credit institution or a financial institution under Section 5, paragraph 1, letter b, points 1 to 10 of the AML/CFT Act which operates in the territory of an EU Member State.
Conclusion	The Slovak law allows the relying on CDD data provided by credit or financial institutions only from EU Member States.
Recommendations and Comments	N/A

11.	**Auditors, accountants and tax advisors**
Art. 2 (1)(3)(a) of the Directive	CDD and record-keeping obligations are applicable to auditors, external accountants and tax advisors acting in the exercise of their professional activities.
FATF R. 12	CDD and record-keeping obligations 1. do not apply to auditors and tax advisors; 2. apply to accountants when they prepare for or carry out transactions for their client concerning the following activities: • buying and selling of real estate; • managing of client money, securities or other assets; • management of bank, savings or securities accounts; • organisation of contributions for the creation, operation or management of companies; • creation, operation or management of legal persons or arrangements, and buying and selling of business entities (2004 AML/CFT Methodology criterion 12.1(d)).
Key elements	The scope of the Directive is wider than that of the FATF standards but does not necessarily cover all the activities of accountants as described by criterion 12.1(d). Please explain the extent of the scope of CDD and reporting obligations for auditors, external accountants and tax advisors.
Description and Analysis	According to Section 5 of the AML/CFT Act auditors, external accountants and tax advisors are obliged entities, and subject to full range of obligation arising from the provisions of the said act. Section 23 of the AML/CFT Act, however, waves their reporting responsibilities when they defend the customer in criminal law proceeding or represent the customer in court proceedings.
Conclusion	The extent and scope of CDD obligations for auditors, external accountants and tax advisors is in line with the Directive. Reporting obligations are limited.
Recommendations and Comments	N/A

12.	**High Value Dealers**
Art. 2(1)(3)e) of the Directive	The Directive applies to natural and legal persons trading in goods where payments are made in cash in an amount of €15 000 or more.
FATF R. 12	The application is limited to those dealing in precious metals and precious stones.
Key elements	The scope of the Directive is broader. Is the broader approach adopted in your jurisdiction?
Description and Analysis	Paragraph 3 of Section 5 of the AML/CFT Act implements Article 2(1)(3)(e) of the Directive to the Slovak Law.
Conclusion	Slovakia has adopted a broader approach then the requirements of R.12
Recommendations and	N/A

Comments	

13.	**Casinos**
Art. 10 of the Directive	Member States shall require that all casino customers be identified and their identity verified if they purchase or exchange gambling chips with a value of €2,000 or more. This is not required if they are identified at entry.
FATF R. 16	The identity of a customer has to be established and verified when he or she engages in financial transactions equal to or above €3,000.
Key elements	In what situations do customers of casinos have to be identified? What is the applicable transaction threshold in your jurisdiction for identification of financial transactions by casino customers?
Description and Analysis	Identification of a customer and verification of his identity are also required in case of carrying out a transaction that amount to at least €2,000, which is also applied to gambling operators and situation in which a client purchases or exchanges gambling chips with a value of €2,000.
Conclusion	The Slovak law is in line with Article 10 of the Directive.
Recommendations and Comments	

14.	**Reporting by accountants, auditors, tax advisors, notaries and other independent legal professionals via a self-regulatory body to the FIU**
Art. 23 (1) of the Directive	This article provides an option for accountants, auditors and tax advisors, and for notaries and other independent legal professionals to report through a self-regulatory body, which shall forward STRs to the FIU promptly and unfiltered.
FATF Recommendations	The FATF Recommendations do not provide for such an option.
Key elements	Does the country make use of the option as provided for by Art. 23 (1) of the Directive?
Description and Analysis	The AML/CFT Act does not provide accountants, auditors and tax advisors, and for notaries and other independent legal professionals with a possibility to report STR through a self regulator body.
Conclusion	The Slovak Law does not implement Article 23 (1) of the Directive.
Recommendations and Comments	The Slovak authorities may wish to consider allowing accountants, auditors and tax advisors, and for notaries and other independent legal professionals to report through a self-regulatory body, which shall forward STRs to the FIU promptly and unfiltered.

15.	**Reporting obligations**
Arts. 22 and 24 of the Directive	The Directive requires reporting where an institution knows, suspects, or has reasonable grounds to suspect money laundering or terrorist financing (Art. 22). Obliged persons should refrain from carrying out a transaction knowing or suspecting it to be related to money laundering or terrorist financing and to report it to the FIU, which can stop the transaction. If to refrain is impossible or could frustrate an investigation, obliged persons are required to report to the FIU immediately afterwards (Art. 24).
FATF R. 13	Imposes a reporting obligation where there is suspicion that funds are the proceeds of a criminal activity or related to terrorist financing.
Key elements	What triggers a reporting obligation? Does the legal framework

	address *ex ante* reporting (Art. 24 of the Directive)?
Description and Analysis	Section 16 of the AML/CFT Act requires the obliged entities to postpone an unusual transaction, as defined by Section 4 of the said act. Ex ante reporting is also covered by the Slovak Law. Triggers for reporting are contingencies stated in an open catalogue form in Section 4 of the Act.
Conclusion	Articles 22 and 24 of the Directive have been implemented in the Slovak Law.
Recommendations and Comments	N/A

16.	**Tipping off (1)**
Art. 27 of the Directive	Art. 27 provides for an obligation for Member States to protect employees of reporting institutions from being exposed to threats or hostile actions.
FATF R. 14	No corresponding requirement (directors, officers and employees shall be protected by legal provisions from criminal and civil liability for "tipping off", which is reflected in Art. 26 of the Directive)
Key elements	Is Art. 27 of the Directive implemented in your jurisdiction?
Description and Analysis	The only provision which may be considered as protecting the employees from being exposed to threats or hostile actions for filing a UTR, are Section 17 para 4: "An unusual transaction report must not include data about the employee who detected the unusual transaction.", and Section 20 para 2 stating that the institutions individual programme must contain the manner of ensuring the protection of employees who detect unusual transactions" It is, however, unclear whether there are other legal mechanisms which would protect the employee from threats or hostile actions.
Conclusion	The provisions of the Slovak Law may be deemed broadly in line with the third AML/CFT Directive.
Recommendations and Comments	The Slovak authorities may wish to analyse if the overall legal framework provides for proper employees protection in line with Article 27 of the Directive.

17.	**Tipping off (2)**
Art. 28 of the Directive	The prohibition on tipping off is extended to where a money laundering or terrorist financing investigation is being or may be carried out. The Directive lays down instances where the prohibition is lifted.
FATF R. 14	The obligation under R. 14 covers the fact that an STR or related information is reported or provided to the FIU.
Key elements	Under what circumstances are the tipping off obligations applied? Are there exceptions?
Description and Analysis	Section 31 of the AML/CFT Act states "Obliged entity, employee of obliged entity, as well as person acting on behalf of obliged entity on the basis of another contractual relationship, shall be obliged to keep secret about reported unusual transaction and measures being taken by the Financial Intelligence Unit in relation to third persons including persons to whom such information relates."
Conclusion	Section 31 of the AML/CFT Act is broadly in line with the third AML/CFT Directive, however the exception provided for in the third to fifth paragraphs of Article 28 of the Third EU AML/CFT Directive are

	not implemented in the Slovak Law
Recommendations and Comments	Slovak authorities may wish to consider including further exceptions as stated in Article 28 of the third AML/CFT Directive.

18.	**Branches and subsidiaries (1)**
Art. 34 (2) of the Directive	The Directive requires credit and financial institutions to communicate the relevant internal policies and procedures where applicable on CDD, reporting, record-keeping, internal control, risk assessment, risk management, compliance management and communication to branches and majority owned subsidiaries in third (non EU) countries.
FATF R. 15 and 22	The obligations under the FATF 40 require a broader and higher standard but do not provide for the obligations contemplated by Art. 34 (2) of the EU Directive.
Key elements	Is there an obligation as provided for by Art. 34 (2) of the Directive?
Description and Analysis	As mentioned previously in this report Slovak AML/CFT Act (Section 24) requires credit and financial institutions to communicate their internal procedures to majority-owned subsidiaries and branches. There is, however, no obligation to require a broader or higher standard.
Conclusion	Obligation stated in article 34 (2) of the Directive was implemented in the Slovak Law.
Recommendations and Comments	N/A

19.	**Branches and subsidiaries (2)**
Art. 31(3) of the Directive	The Directive requires that where legislation of a third country does not permit the application of equivalent AML/CFT measures, credit and financial institutions should take additional measures to effectively handle the risk of money laundering and terrorist financing.
FATF R. 22 and 21	Requires financial institutions to inform their competent authorities in such circumstances.
Key elements	What, if any, additional measures are your financial institutions obliged to take in circumstances where the legislation of a third country does not permit the application of equivalent AML/CFT measures by foreign branches of your financial institutions?
Description and Analysis	According to Section 24 of the AML/CFT Act, should the legislation of a third country not permit application of measures equivalent to those set out in Slovak Law, the obliged entity shall inform the FIU about it and take additional measures to prevent ML and TF. No specific catalogue of additional measures as mentioned in the said section was established.
Conclusion	Article 31 (3) of the Directive is implemented in the Slovak Law
Recommendations and Comments	Slovak authorities may wish to consider establishing a catalogue (in guidelines) of additional measures which should be taken by credit or financial institutions in situation stipulated in Section 24 of the AML/CFT Act.

20	**Supervisory Bodies**
Art. 25 (1) of the Directive	The Directive imposes an obligation on supervisory bodies to inform the FIU where, in the course of their work, they encounter facts that could contribute evidence of money laundering or terrorist financing.
FATF R.	No corresponding obligation.

Key elements	Is Art. 25(1) of the Directive implemented in your jurisdiction?
Description and Analysis	Section 31 of the AML/CFT Act does provide for the obligation set out in Article 25(1) of the Third EU AML/CFT Directive.
Conclusion	The Slovak law is compliant in this matter with the Third EU AML/CFT Directive.
Recommendations and Comments	N/A

21	**Systems to respond to competent authorities**
Art. 32 of the Directive	The Directive requires credit and financial institutions to have systems in place that enable them to respond fully and promptly to enquires from the FIU or other authorities as to whether they maintain, or whether during the previous five years they have maintained, a business relationship with a specified natural or legal person.
FATF R.	There is no explicit corresponding requirement but such a requirement can be broadly inferred from Recommendations 23 and 26 to 32.
Key elements	Are credit and financial institutions required to have such systems in place and effectively applied?
Description and Analysis	Paragraph 4 of Section 24 of the Slovak AML/CFT Act clearly states an obligation as set out in Article 32 of the Third EU AML/CFT Directive.
Conclusion	The Slovak Law follows the obligation of Article 32 of the third AML/CFT Directive.
Recommendations and Comments	N/A

22	**Extension to other professions and undertakings**
Art. 4 of the Directive	The Directive imposes a *mandatory* obligation on Member States to extend its provisions to other professionals and categories of undertakings other than those referred to in A.2(1) of the Directive, which engage in activities which are particularly likely to be used for money laundering or terrorist financing purposes.
FATF R. 20	Requires countries only to consider such extensions.
Key elements	Has your country implemented the mandatory requirement in Art. 4 of the Directive to extend AML/CFT obligations to other professionals and categories of undertaking which are likely to be used for money laundering or terrorist financing purposes? Has a risk assessment been undertaken in this regard?
Description and Analysis	The catalogue of obliged entities under Section 5 of the AML/CFT Act comprise for instance: "a postal undertaking, a court distrainer, an administrator who manages activity within bankruptcy, restructuring proceedings or debt removal proceedings under a special regulation, a legal entity or a natural person authorised to provide the services of organisational and economic advisor, the services of public carriers and messengers or forwarding services, and other person if so laid down by a special regulation." The said catalogue is broad, and the evaluation team was made aware that it was being considered what kind of specific entity should be listed as obliged entity. There is however no written risk assessment in this matter.
Conclusion	Slovakia has implemented the mandatory requirement in Art. 4 of the Directive to extend AML/CFT obligations to other professionals and categories of undertakings which are likely to be used for money laundering or terrorist financing purposes. However, no formal risk assessment has been undertaken in this regard.

Recommendations and Comments	It is recommended that a formal risk assessment is carried out to determine which professional categories other than those specified in Section 5 of the AML/CFT Act are likely to be used for ML or TF purposes.

23	**Specific provisions concerning equivalent third countries?**
Art. 11, 16(1)(b), 28(4),(5) of the Directive	The Directive provides specific provisions concerning countries which impose requirements equivalent to those laid down in the Directive (e.g. simplified CDD).
FATF R.	There is no explicit corresponding provision in the FATF 40 plus 9 Recommendations.
Key elements	How, if at all, does your country address the issue of equivalent third countries?
Description and Analysis	Under the provisions of Slovak Law there is a presumption of equivalence between financial institutions from Slovakia, EU\EEA countries and third countries as set out in the AML/CFT Act. This presumption translates into specific exemptions in the CDD measures for instance. The only binding third countries list as at time of the on-site visit was the one of the EU.
Conclusion	Slovak provisions on equivalent third countries correspond to those in the third AML/CFT Directive.
Recommendations and Comments	N/A

VI. ANNEXES

See MONEYVAL(2011)21ANN