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

MONEYVAL(2017)2

Anti-money laundering and counter-terrorist financing measures

Slovenia

Fifth Round Mutual Evaluation Report

June 2017

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

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

The fifth round mutual evaluation report on Slovenia was adopted by the MONEYVAL Committee at its 53rd Plenary Session (Strasbourg, 1 June 2017).

TABLE OF CONTENTS

EXECUTIVE SUMMARY 7
A. Key Findings 7
B. Risks and General Situation 9
C. Overall Level of Effectiveness and Technical Compliance 9
D. Priority Actions 14
E. Effectiveness and Technical Compliance Ratings 15

MUTUAL EVALUATION REPORT 16
Preface 16

CHAPTER 1. ML/FT RISKS AND CONTEXT 17
ML/FT Risks and Scoping of Higher-Risk Issues 17
Country's risk assessment 21
AML/CFT Strategy 24
Legal framework 24
Institutional Framework 24
Financial sector and DNFBPs 26
Preventive measures 28
Legal persons and arrangements 29
Supervisory arrangements 30
International Cooperation 33

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION 34
Key Findings and Recommended Actions 34
Immediate Outcome 1 (Risk, Policy and Coordination) 35

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES 44
Key Findings and Recommended Actions 44
Immediate Outcome 6 (Financial intelligence ML/FT) 47
Immediate Outcome 7 (ML investigation and prosecution) 57
Immediate Outcome 8 (Confiscation) 67

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION 76
Key Findings and Recommended Actions 76
Immediate Outcome 9 (TF investigation and prosecution) 78
Immediate Outcome 10 (TF preventive measures and financial sanctions) 84
Immediate Outcome 11 (PF financial sanctions) 90

CHAPTER 5. PREVENTIVE MEASURES 92
Key Findings and Recommended Actions 92
Immediate Outcome 4 (Preventive Measures) 93

CHAPTER 6. SUPERVISION 103
Key Findings and Recommended Actions 103
Immediate Outcome 3 (Supervision) 104

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS 116
Key Findings and Recommended Actions 116

Immediate Outcome 5 (Legal Persons and Arrangements) 117

CHAPTER 8. INTERNATIONAL COOPERATION 125
Key Findings and Recommended Actions 125
Immediate Outcome 2 (International Cooperation) 126

TECHNICAL COMPLIANCE ANNEX 138
Recommendation 1 - Assessing Risks and applying a Risk-Based Approach 138
Recommendation 2 - National Cooperation and Coordination 141
Recommendation 3 - Money laundering offence 142
Recommendation 4 - Confiscation and provisional measures 145
Recommendation 5 - Terrorist financing offence 147
Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing 149
Recommendation 7 – Targeted financial sanctions related to proliferation 153
Recommendation 8 – Non-profit organisations 156
Recommendation 9 – Financial institution secrecy laws 159
Recommendation 10 – Customer due diligence 160
Recommendation 11 – Record-keeping 163
Recommendation 12 – Politically exposed persons 164
Recommendation 13 – Correspondent banking 166
Recommendation 14 – Money or value transfer services 167
Recommendation 15 – New technologies 168
Recommendation 16 – Wire transfers 169
Recommendation 17 – Reliance on third parties 171
Recommendation 18 – Internal controls and foreign branches and subsidiaries 172
Recommendation 19 – Higher-risk countries 174
Recommendation 20 – Reporting of suspicious transaction 174
Recommendation 21 – Tipping-off and confidentiality 175
Recommendation 22 – DNFBPs: Customer due diligence 176
Recommendation 23 – DNFBPs: Other measures 177
Recommendation 24 – Transparency and beneficial ownership of legal persons 178
Recommendation 25 – Transparency and beneficial ownership of legal arrangements 185
Recommendation 26 – Regulation and supervision of FIs 188
Recommendation 27 – Powers of supervisors 189
Recommendation 28 – Regulation and supervision of DNFBPs 191
Recommendation 29 - Financial intelligence units 192
Recommendation 30 – Responsibilities of law enforcement and investigative authorities 194
Recommendation 31 - Powers of law enforcement and investigative authorities 196
Recommendation 32 – Cash Couriers 198
Recommendation 33 – Statistics 200
Recommendation 34 – Guidance and feedback 201
Recommendation 35 – Sanctions 201
Recommendation 36 – International instruments 202
Recommendation 37 - Mutual legal assistance 203
Recommendation 38 – Mutual legal assistance: freezing and confiscation 205
Recommendation 39 – Extradition 206
Recommendation 40 – Other forms of international cooperation 208

LIST OF ABBREVIATIONS

ACCMEU	Act on Cooperation in Criminal Matters with the Member States of the European Union
APLRRS	Agency for Public Legal Records and Related Services
APMLFT	Act on the Prevention of Money Laundering and Financing of Terrorism
APOA	Agency for Public Oversight of Auditing
ARM	Act on Restrictive Measures
BoS	Bank of Slovenia
CAS	Chamber of Accounting Services
CC	Criminal Code
CCIS	Chamber of Commerce and Industry of Slovenia
CDD	Customer Due Diligence
CEVS	Counterterrorism and Extreme Violence Section
CFT	Combating the Financing of Terrorism
CISCDNGOs	Centre for Information Service, Co-operation and Development of NGOs
CLLEA	Criminal Liability of Legal Entities Act
CSCC	Central Securities Clearing Corporation
DNFBP	Designated Non-Financial Business or Profession
EC	European Commission
ECB	European Central Bank
ELIC	Expert and Legal Information Centre
EU	European Union
FAIOA	Forfeiture of Assets of Illegal Origin Act
FARS	Financial Administration of the Republic of Slovenia
FATF	Financial Action Task Force
FCMLS	Financial Crime and Money Laundering Section
FIMA	Financial Instruments Market Act
FIs	Financial institutions
FIU	Financial Intelligence Unit
GDP	Gross Domestic Product
IA	Insurance Act
IFCA	Investment Funds and Companies Act
INTERPOL	International Police
IO	Immediate Outcomes
IOSCO	International Organisation of Securities Commissions
ISA	Insurance Supervision Agency
LEA	Law enforcement agencies
LLPCOA	Liability of Legal Persons for Criminal Offences Act
MJ	Ministry of Justice
MF	Ministry of Finance
MFA	Ministry of Foreign Affairs
MI	Ministry of Interior
MIRS	Market Inspectorate of the Republic of Slovenia
ML	Money Laundering
MLA	Mutual Legal Assistance
MOU	Memorandum of Understanding
MVTS	Money or Value Transfer Services

NBI	National Bureau of Investigation
NGO	Non-Governmental Organization
NPO	Non-Profit Organization
NRA	National Risk Assessment
OECD	Organisation for Economic Co-operation and Development
OMLP	Office for Money Laundering Prevention
ORSGS	Office of the Republic of Slovenia for Gaming Supervision
PEP	Politically Exposed Person
PF	Proliferation Financing
PSP	Payment service provider
SAR	Suspicious Activity Report
SIA	Slovenian Institute of Auditors
SIS	Schengen Information System
SMA	Securities Market Agency
TF	Terrorist Financing
TFS	Targeted financial sanctions
TIEA	Tax Information Exchange Agreements
TCSP	Trust and Corporate Service Providers
STR	Suspicious Transaction Report
UN	United Nations
UNSCR	United Nations Security Council Resolution

EXECUTIVE SUMMARY

1. This report provides a summary of the anti-money laundering and combating the financing of terrorism (AML/CFT) measures in place in Slovenia as at the date of the on-site visit. It analyses the level of compliance with the Financial Action task Force (FATF) 40 Recommendations and the level of effectiveness of Slovenia's AML/CFT system, and provides recommendations on how the system could be strengthened.

A. Key Findings

1. The authorities have partially succeeded in identifying, assessing, and understanding money laundering (ML) risks. This has been primarily done through the first national risk assessment (NRA) of 2015 and the updated NRA of 2016. There is, however, a mixed understanding of ML risks among competent authorities and the private sector. Financing of terrorism (FT) risks were only assessed to a very limited extent in the two NRAs, and the overall understanding of FT risks varies significantly between different stakeholders.
2. Various platforms and mechanisms are in place to support coordination of AML/CFT and CPF policy-making and operational work. These have, however, not yet been effectively exploited to coordinate and implement policies on a risk-sensitive basis. The recently adopted Action Plan, based on the results of the updated NRA, forms a good starting point to improve the AML/CFT regime, although its potential may be undermined by rather general, and ambiguously set, objectives and activities.
3. Financial intelligence gathered by the Slovenian financial intelligence unit (OMLP) has been used to some extent by the law enforcement agencies (LEAs) to investigate and prosecute ML. Although LEAs develop evidence and trace criminal proceeds in ML cases based on this intelligence, the effectiveness of its use in ML and predicate offence related investigations is strongly influenced by legal, jurisprudential and contextual factors related to Slovenia and its overall AML/CFT system.
4. Although the number of ML investigations has risen, it is not commensurate with the number of investigations and convictions for proceeds generating predicate offences. Slovenia's risk profile would warrant a higher number of ML investigations related to serious crimes. Progress in securing ML convictions, including in relation to third-party ML and autonomous ML, has been achieved. Nevertheless, a number of obstacles hinder the prosecution and adjudication of ML cases, including: uncertainty as to the evidentiary requirements in proving ML and the underlying predicate offence; judges' and prosecutors' insufficient expertise on financial forensics/crimes, and; in relation to ML cases in which the underlying predicate crime has been committed in a neighbouring jurisdiction.
5. Confiscation of proceeds is mandatory as per respective criminal legislation. The absence of 'extended confiscation' in criminal proceedings was remedied by introduction of the civil confiscation regime. However, it has, so far, produced only limited results given concerns raised before the Constitutional Court with regard to human rights considerations.
6. Several good examples of international cooperation demonstrate that Slovenia proactively seeks mutual legal assistance (MLA), including in areas of increased risk, and has achieved relevant results. There are also some successful cases of international cooperation in relation to incoming MLA requests, which have resulted in convictions and confiscation of property. The OMLP and LEA actively engage in international cooperation, request assistance from foreign counterparts and provide timely and good quality assistance to competent authorities from other countries (both European Union (EU) and non-EU). Difficulties experienced by the OMLP in receiving information from a counterpart in a neighbouring country on specific typology has hampered the effective elaboration/use of intelligence and the opening of ML investigations in relation to this typology.

7. Banks have a sound understanding of the major sector-specific ML risks, and mitigating measures applied are largely commensurate. The situation varies among non-bank FIs, while DNFBPs lack awareness of the extent to which they are exposed to ML risks. Implementation of CDD requirements by FIs has improved substantially over recent years; however, significant gaps exist in the DNFBP sectors (e.g. real estate and notaries). The OMLP is generally satisfied with the quality of STRs received from banks, but reports from non-bank FIs lack meaningful information. The level of reporting among DNFBPs is inadequately low considering their involvement with higher-risk customers and products. FT-related reports are rare and mostly submitted by larger banks.

8. Supervisors are effective in preventing convicted criminals having control of, or management positions in, obliged entities. However, there is concern regarding supervisors' ability to detect and prevent people with a criminal background and their associates gaining ownership or management positions in these institutions. With regard to DNFBPs and FIs other than banks, payment and e-money institutions, insurance and securities companies, there is no on-going mechanism to check the fit and proper status of those individuals that have already been authorised.

9. Whilst both NRAs have improved the understanding of financial services supervisors of the risks in their sectors, there is no on-going mechanism for cooperation amongst supervisors and with the OMLP to promote a better understanding of the risks on a national and sectorial level. The department of the Bank of Slovenia (BoS) responsible for banking supervision has a good understanding of the sector risk of ML and specific risks of the banks under its supervision. However, other supervisors have a lower level of understanding of ML risks. All supervisors have limited understanding and knowledge regarding specific FT issues in their area of responsibility.

10. The BoS has adopted a risk-based approach to ML/FT supervision that takes relevant parameters into account. Other supervisors have no-risk based approach to supervision for ML/FT issues and the OMLP has not yet developed a strategy for using its newly acquired supervisory powers.

11. The law enforcement and intelligence authorities have a good understanding of FT risks. They proactively exchange information on suspicions of FT in the pre-investigative phase. They are also vigilant to the potential for abuse of NPOs for FT. However, the limited FT offence appears to hinder their ability to properly investigate and prosecute all forms of FT. Furthermore, Slovenia has not undertaken a domestic review of the NPO sector to identify which parts might be at particular risk of being misused for FT, and no risk-based supervision of NPOs is in place.

12. Targeted financial sanctions (TFS) imposed by the United Nations against FT and PF are not implemented without delay due to reliance placed on the EU legal framework. There is basic awareness about TFS among most FIs but not among DNFBPs. The Sanctions Coordination Group (SCG) forms a suitable platform to coordinate and promote the implementation of TFS, but limited resources appear to have hampered its effective use.

13. Competent authorities rely on obliged entities to obtain information on the beneficial ownership of legal persons. Although DNFBPs involved in company formation do not adequately fulfil their gatekeeper role, the majority of Slovenian companies have a bank account in Slovenia, and banks demonstrated compliance with beneficial ownership obligations to a considerable extent. Slovenia has undertaken certain measures to increase transparency of legal persons and prevent their misuse, but these measures have not proven sufficient to effectively prevent criminals from setting up companies for illicit purposes making use of "front men".

B. Risks and General Situation

2. Slovenia is not a major international financial centre and does not have high domestic crime rates; nonetheless, its relatively stable and reliable financial sector may attract money launderers from around the region. The level of financial inclusion is very high: approximately 97% of the population holds a bank account.[1] The share of non-residents in the overall customer base is estimated at 2.2% among natural persons and 0.8% among legal entities with comparable turnover figures. The banking sector accounts for the largest part of the financial services industry in Slovenia and is deemed most vulnerable to ML. A significant proportion of transactions carried out by non-bank FIs and their customers go through the banking system as the use of cash transfers is relatively low in Slovenia and cash payments for goods and services exceeding EUR 5,000 are prohibited. Financial institutions other than banks are not deemed particularly vulnerable to ML, and the NRAs rate several DNFBP sectors as presenting a medium vulnerability for ML.

3. According to the NRAs, the domestic economic crime offences which are deemed to pose the highest ML threat are abuse of position or trust in the performance of economic activities, tax evasion, business fraud and abuse of official position or official duties. Outside the realm of economic crime, offences related to illicit drugs are deemed to pose the highest ML threat. Slovenia's geographical position between the EU and the Balkans exposes it to external threats, including, in particular, drug trafficking. ML investigations are mostly linked to the investigation of criminal offences in the field of economic crime, and, to a lesser extent, to the areas of organised crime, corruption and general criminality.

4. Slovenia's geographic situation is relevant when considering the risks of terrorism and financing of terrorism that the country faces. Neighbouring countries in the Balkan region have seen a strong rise in terrorism risks in the aftermath of past regional conflicts, originating from separatist groups. Recently, the wider region has experienced an increase in Islamist radicalisation and nationals joining the so-called Islamic State (ISIS) as foreign fighters in Syria and Iraq. Slovenia itself reportedly has "little to no experience" with terrorism or the financing of terrorism. According to the NRAs, information from the interministerial Working Group for Combating Terrorism, operating within the National Security Council, does not reveal any serious threats. Nevertheless, as indicated in the NRAs, there are suspicions that 10 people have left Slovenia to go to Syria or Iraq, and there is some recent information indicating activities in the field of training and recruitment for terrorist activities and promotion of radicalisation. Outside the context of radical Islamist terrorism, Slovenia has experienced one recent case of attempted terrorist acts.

C. Overall Level of Effectiveness and Technical Compliance

5. Following the last evaluation in 2010, the Slovenian AML/CFT regime has undergone important changes. Slovenia completed its first NRA in 2015 using the National Money Laundering and Terrorist Financing Risk Assessment Tool provided by the World Bank, and adopted an updated version of the NRA and Action Plan (the latter based on the updated version of NRA) in 2016. Key institutions such as the specialized prosecutor's offices and police divisions for complex economic crime and the Commission for the Prevention of Corruption (CPC) have been established or strengthened in recent years in order to prevent and fight corruption. The legislative framework was strengthened with the adoption of the Act on the Prevention of Money Laundering and the Financing of Terrorism (APMLFT) which replaces earlier legislation in force since 2008. The legal framework in Slovenia is broadly in line with the requirements of the FATF standards, with a few notable exceptions. The structural elements needed to ensure an effective AML/CFT system are generally present in Slovenia, including political and institutional stability, accountable institutions and the rule of law.

[1] World Bank, *The Global Findex Database 2014 – Measuring Financial Inclusion around the World,* 2014.

6. In terms of effectiveness, Slovenia has demonstrated substantial results with respect to Immediate Outcome (IO.2) and moderate effectiveness with respect to ten Immediate Outcomes (IO.1 and 3-11).

C.1 Assessment of Risks, Coordination and Policy Setting (Chapter 2 - IO.1; R.1, R.2, R.33)

7. The authorities have partially succeeded in identifying, assessing, and understanding ML risks. This is primarily done through the NRAs of 2015 and 2016. Domestic threats (and to a limited extent cross-border threats) and vulnerabilities in the national system and in the financial and non-financial sectors were considered. The NRAs show some weaknesses related to sources of information and integration of results of the threat and vulnerability assessments to arrive at a common understanding of the most important risks. Furthermore, they contain only a very limited analysis of FT risks. Communication with the private sector should be strengthened to increase their level of understanding of the national risks, especially with regard to FT.

8. The OMLP is considered to be the key AML/CFT authority in the development and implementation of AML/CFT policies and activities. Additionally, there are numerous interagency working groups, committees and mechanisms to facilitate policy-making and operational coordination. They have not yet led to sufficient ML/FT risk-sensitive allocation of resources among all relevant authorities, and their use to coordinate AML/CFT policy-making could be strengthened. Operational cooperation between the competent authorities is in most cases effective. However, there are some areas where further improvements are needed, especially with regard to communication between supervisors and coordination of implementation of FT and PF TFS.

9. The OMLP will be mainly responsible for coordinating the implementation of the AML/CFT Action Plan, which was elaborated based on the updated NRA and adopted by the government in late 2016. The Action Plan appears a good starting point for further improvement of measures to mitigate the AML/CFT risks, although its objectives and activities are not always clearly articulated.

C.2 Financial Intelligence, Money Laundering and Confiscation (Chapter 3 - IOs 6-8; R.3, R.4, R.29-32)

10. Financial intelligence in Slovenia derives from a range of information collected by the OMLP. The OMLP has access, directly or indirectly, to a broad range of financial, commercial, real estate, tax and customs information. The OMLP is proactive in seeking relevant financial and other information as well as in assisting authorities to obtain data needed in their pre-investigative and investigative activities related to ML/FT and proceeds generating crimes.

11. Although the quality of financial intelligence and the level of cooperation between the OMLP and LEAs are considered to be high, statistics show that the actual use of intelligence to investigate and prosecute ML is relatively low. This is primarily due to the standards of proof set by the jurisprudence and the respective laws, which the OMLP and LEAs perceive as considerably high. On the other hand, OMLP powers in gathering financial data have been used by LEAs and the intelligence service whenever there was a reasonable doubt that a terrorist attack would be committed. However, a FT offence was not identified in any of these cases.

12. Although the number of ML investigations has steadily risen, it is not commensurate with the number of investigations and convictions for proceeds generating predicate offences, as parallel financial investigations are not conducted systematically. ML investigations and prosecutions reflect, to some extent, the risks that the country faces, however, Slovenia's risk profile would warrant a higher number of ML investigations related to foreign tax predicate offences, corruption offences, drug offences and organised criminality. Progress has been achieved in securing ML convictions, including in relation to third-party ML and autonomous ML, yet a number of obstacles to prosecuting and adjudicating ML cases need to be tackled in order to significantly improve the system, notably: uncertainty as to the evidentiary requirements in proving ML and the underlying predicate offence; judges' and prosecutors' insufficient expertise on financial forensics/crimes, as well as insufficient administrative personnel; and in relation to ML cases in which the underlying predicate crime has been committed in a neighbouring jurisdiction. Custodial sentences which have been imposed are at

the lower end of the "sanctioning" scale and the fines imposed on legal persons have been too lenient.

13. The relevant strategies confirm that the confiscation of proceeds of crime is taken as a priority at both strategic and operational levels. However, this has not been sufficiently pursued in practice. Although the legislative framework is comprehensive, the actual amount of confiscated property suggests that its application suffers from different factors. These factors primarily concern non-systematic application of parallel financial investigations for all profit generating crimes, absence of specialised institutions responsible for management of assets, low level of execution of actual confiscation decisions and underused asset sharing mechanisms. The civil confiscation regime has so far produced only limited results. The majority of cases are still before the Constitutional Court awaiting its decisions on constitutionality of the law – an issue raised by those whose property was under scrutiny.

14. The confiscation at the border of falsely declared or undeclared cash and bearer negotiable instruments (BNIs) that are suspected to relate to ML/FT and associated predicate offences has not been implemented in practice so far. In addition, the declaration system with regard to cross-border transportation of currency and other financial instruments does not apply to movements of BNI and cash within the EU.

C.3. Terrorist Financing and Financing Proliferation (Chapter 4 - IOs 9-11; R.5-8)

15. Slovenia has incorporated a very limited analysis of FT risks into its NRAs. Key authorities nevertheless showed satisfactory understanding of current FT risks. Although the FT risks in Slovenia are relatively low, the possibilities for FT activity cannot be understated and should be dealt with vigilantly.

16. Slovenia has an institutional framework in place to investigate and prosecute FT. LEAs and intelligence agencies are aware of current risks, pay due regard to suspicions of FT and make use of available (pre-) investigative methods. Annually, the police deal with five to ten cases that have certain indications of FT. The authorities have not yet proceeded to formal investigations of FT. The gaps in the FT offence appear to have negative repercussions on their abilities to pursue FT and must be remedied urgently. Furthermore, the lack of communication on FT risks to all relevant stakeholders and the lack of a national CFT strategy are believed to undermine effective detection and pursuit.

17. Slovenia has established a coordination group for the implementation of targeted financial sanctions. The group includes all relevant stakeholders and provides a suitable platform for information exchange and cooperation between authorities, but suffers from limited resources. Guidance provided to obliged entities is limited. FIs met on-site demonstrated only a basic level of awareness of the implementation of TFS; and DNFBPs were generally unaware of their existence. The authorities did not demonstrate adequate supervision of the implementation of TFS.

18. Slovenia relies on EU measures of implementation for UNSCR 1267 and subsequent resolutions, as well as EU implementation of UNSCR 1373, with some national complementing measures (primarily by establishing fines for violations of sanctions obligations). This reliance creates delays in implementation of UNSCR 1267. Although the national law gives the Slovenian government powers to adopt national regulations transposing UN designations while awaiting EU implementation, these have not been used in practice. No motions have been made for designation of persons to the UN or EU lists, nor have designations at the domestic level been considered. No freezing of funds or other assets has taken place. The lack of awareness among FIs and DNFBPs and the delays in implementation of sanctions are concerning in light of the increased risks for FT globally and in the region.

19. Authorities have made important efforts to increase transparency in the NPO sector, and there are good frameworks in place to obtain information on their structures and extend oversight over their funding sources. NPOs met on-site were, in general, aware of their obligations and aware of their possible abuse for illicit activities thanks to internal rules. LEAs and intelligence agencies are

sufficiently vigilant to the FT risks of NPOs and take coordinated mitigating actions. On the other hand, no in-depth assessment of risks for FT abuse in the sector has taken place, and no risk-based approach to supervision of NPOs is in place.

C.4 Preventive Measures (Chapter 5 - IO4; R.9-23)

20. Banks demonstrated a proactive assessment and consideration of major sectorial ML risks, while the situation varies among non-bank FIs. The understanding of ML risks is significantly less well developed among DNFBPs compared to the financial sector. Although, the awareness of FT risks is generally low across all sectors, larger banks did demonstrate a relatively higher understanding, but lack guidance from the authorities to apply sufficient risk-mitigating measures.

21. All FIs apply a basic risked-based approach and implement certain elements of enhanced CDD in relation to customers classified as higher risk. However, checks done by banks are more extensive and elaborate. Although every obliged entity is required to analyse ML/FT risks in its activities and act accordingly, DNFBPs rarely apply the risk-based approach to business relationships. Some of the DNFBPs met on-site stressed that they usually rely on banks to mitigate ML/FT risks.

22. There are some concerns about the depth and consistency of the verification of beneficial owners of customers by FIs (particularly for non-bank FIs). The requirements of the APMLFT have until very recently applied to only foreign PEPs who are treated as higher-risk customers by all FIs. The majority of banks met on-site demonstrated existence of appropriate risk-management systems to ascertain PEPs, but only one bank claimed that it has also been identifying domestic PEPs. Among DNFBPs, only casinos showed a degree of awareness of the requirements related to PEPs. FIs demonstrated a basic level of awareness of FT-related TFS, but their implementation is hindered by delays in the transposition of UNSCR lists into the EU legislation. DNFBPs interviewed were generally unaware of the existence of TFS. The awareness of the correspondent banking requirements and the FATF list of higher-risk jurisdictions is high among FIs. DNFBPs met on-site were generally unaware about the latter.

23. The number of STRs has been steadily increasing over the years, yet the vast majority of reports are submitted by banks. OMLP expressed satisfaction with the quality of most of the STRs received. The inadequate level of reporting among DNFBPs seems to be the consequence of limited awareness of reporting requirements. FIs are well aware of their record-keeping obligations and maintaining customer identification data, account files and business correspondence is the norm. The supervisory authorities have not identified any serious deficiencies in this respect. No issues have been raised regarding the tipping-off prohibition.

24. Banks have sound AML/CFT internal controls in place. While some non-bank FIs demonstrated existence of quite well-organised and professional AML/CFT compliance functions, the application of internal controls in DNFBP sectors appears very limited.

C.5 Supervision (Chapter 6 - IO3; R.26-28, R. 34-35)

25. Supervisors' actions are effective in preventing convicted criminals from being directors and beneficial owners of FIs. Supervisors did not demonstrate effectiveness in their ability to detect and prevent people with a criminal background and their associates gaining ownership or management positions in FIs. At the same time, every bank is required to conduct its own fit and proper tests for board members and employees that hold a key function. Banks' procedures in this regard are subject to BoS supervision. There is no on-going mechanism to check the fit and proper status of those individuals that have already been authorised in the DNFBP sector or for FIs other than banks, payment and e-money institutions, insurance and securities companies.

26. BoS, which is responsible for supervision of the banking sector, has a satisfactory understanding of the ML risks in its supervision of banks and is aware of the prevalent typologies for ML in the national context as well as the methodologies prevalent in banks. However, the lack of regular and systematic sharing of information with the OMLP and other supervisors hampers development of the collective understanding required to effectively identify ML/FT risks. Whilst other financial

supervisors have a general understanding of the level of risk in their areas of responsibility, they lack understanding at the product and customer level. With regards to FT risks, there is an across the board agreement amongst all supervisors and professional bodies that much needs to be done to improve their knowledge of risks in this area.

27. A risk-based approach to AML/CFT supervision has only been adopted by the BoS, whilst other supervisors do not implement such an approach and have no immediate plans to do so. Although the BoS consults the OMLP before every specific inspection, the effectiveness of the risk analysis of banks by BoS could be improved if they were to regularly receive information from the OMLP regarding the quality of STRs and CTRs of all banks.

28. The BoS demonstrated a significant improvement in the level of AML/CFT compliance of banks under its supervision. Whilst there are sanctioning tools available to the BoS, its lack of use of financial sanctions is likely to hamper efforts to further improve banks' commitments.

C.6 Transparency of Legal Persons and Arrangements (Chapter 7 - IO5; R. 24-25)

29. Although Slovenia has not carried out an in-depth analysis of ML/FT vulnerabilities of all types of legal entities which may be established in the country, the authorities have demonstrated an understanding of general vulnerabilities.

30. The availability of basic information on legal entities established in Slovenia through the Business Register is at a high level, although there are some concerns about the effectiveness of existing mechanisms to ensure that the information is accurate and up-to-date. Currently, competent authorities rely on obliged entities to obtain the necessary beneficial ownership information. Although legal entities are not required to have business relations with a domestic obliged entity, the overwhelming majority of companies have a bank account in Slovenia. Banks demonstrated compliance with beneficial ownership requirements to a considerable extent, but some gaps remain in the understanding of indirect control. The new APMLFT has introduced a new obligation for legal persons to discover and maintain information on their beneficial owners and to report this to the Registry on beneficial ownership - envisaged to be operational in 2018.

31. Slovenia has certain mechanisms in place to prevent the misuse of legal entities. Prospective founders, shareholders and managers of companies are subject to criminal background checks, and restrictions were recently imposed on the number of companies that can be set up by one person. However, these measures have not proven sufficient to effectively prevent criminals from setting up companies for illicit purposes making use of "front men" as founder or director.

C.7. International Cooperation (Chapter 8 - IO2; R. 36-40)

32. Slovenia has in place a satisfactory legal framework to provide MLA and service extradition requests. Although the deficiencies in the criminalisation of the FT offence may limit Slovenia's ability to provide MLA or extradite in FT cases in practice, the incomplete criminalisation of terrorist financing has not been an issue. Reliable statistics on MLA and extraditions have not been collected in the period under review. Nonetheless, several good examples of international cooperation have been produced demonstrating that Slovenia proactively seeks MLA from other states in several areas of increased risk, including drug trafficking and organised crime, and has convicted defendants and/or seized and confiscated proceeds as a result. As for incoming requests, a few successful cases of international cooperation have also been presented which have resulted in convictions and confiscation of property.

33. The OMLP and LEAs extensively exchange information with their foreign counterparts. The difficulties experienced by the OMLP in receiving information from a FIU and LEAs in a neighbouring country have hampered the effective elaboration/use of intelligence and the opening of ML investigations in relation to a specific typology. The OMLP, however, has been proactive in trying to resolve this problem. As concerns supervisory authorities, whilst the BoS is active in seeking and providing international cooperation with its counterparts for AML/CFT purposes, the SMA and the MI have not been active in this respect. The weaknesses identified under IO.5 may affect the

authorities' ability to exchange beneficial ownership information in cases of legal persons established in Slovenia by foreign legal entities.

D. Priority Actions

34. The prioritized recommended actions for Slovenia, based on these findings, are:

1. The authorities should ensure a more complete and reliable assessment of ML/FT risks in the country by broadening the types of information used in the risk assessment process, ensuring participation of all relevant stakeholders and covering areas that were overlooked in the first and updated NRA. Special attention should be paid to ensure that the threat and vulnerability assessments result in a joint understanding of ML/FT risks among relevant authorities, which should also proactively communicate information on risks to the private sector.

2. The AML/CFT Action Plan should include clear objectives and activities for the competent authorities that are consistent with the identified ML/FT risks, and allow for risk-sensitive allocation of resources. Intended outcomes of the activities should be specified in order to allow for proper monitoring of their effectiveness. Existing national coordination and cooperation platforms should be used more effectively, in order to ensure and monitor the implementation of AML, CFT and CPF policies and activities and to propose necessary improvements.

3. Slovenia should encourage LEAs to use financial intelligence more proactively in cases where clear indicators on specific predicate offence are missing. In this regard, further guidance and training should be developed for prosecutors and LEAs to enhance the use of financial intelligence for pursuing ML cases in the absence of information on the specific predicate crime.

4. Slovenia should streamline cooperation between LEAs, the OMLP and the FARS on gathering evidence on ML and tracing assets deriving from tax-related criminal offences as a predicate crime.

5. The number of specialised staff performing ML/FT financial intelligence analysis in the OMLP and in the Criminal Police Directorate should be increased and the internal analytical methodology for processing and analysing STRs should be developed.

6. Parallel financial investigations, alongside or in the context of the criminal investigation, should be systematically organised, particularly in serious and complex proceed-generating cases.

7. The authorities should be more proactive in investigating and prosecuting ML related to serious crime, in line with Slovenia's risk profile.

8. Clarity should be shed on the judgments issued in 2014 and 2015 by the Supreme Court, including on the interpretation given on evidential thresholds for establishing the underlying predicate criminality. Training to prosecutors and judges on such evidential thresholds should be provided and prosecutors should present the judiciary with more cases in which the underlying offence(s) is not unequivocally established.

9. Slovenia should establish a legal and institutional framework to ensure the effective and systematic management of assets.

10. Slovenia should improve the statistical system to maintain reliable and detailed data on confiscations in order to analyse effectiveness of asset recovery and consistency of efforts with the country's risk profile.

11. The FT offence should be amended to remedy the identified gaps under R.5 in order to achieve full criminalization of FT as required by the standard and to avoid impediments of the effectiveness of the CFT regime. A national CTF strategy should be developed that clearly outlines the priority actions in the FT field and that formalizes the practice for conducting proactive parallel financial investigations in FT cases.

12. The NPO sector should be assessed to identify those NPOs most at risk for FT abuse, and a risk-based approach to supervision of NPOs should be implemented.

13. Measures should be taken to ensure that TFS are implemented without delay and to increase awareness of TFS among FIs and DNFBPs.

14. Slovenia should improve its assessment of the vulnerabilities and potential for misuse for ML/FT of all types of legal persons which may be established in the country, and should ensure that coordinated measures are taken to mitigate the risks of misuse.

15. Slovenia should ensure that the mechanism to be implemented for obtaining information on beneficial ownership includes sufficient powers and resources for the OMLP to apply verification measures and to ensure that information is accurate, up-to date and available to the competent authorities in a timely manner.

16. Statistics on MLA and extradition, including those made through direct contact, should be collected and should indicate the types of crime which they relate to, as well as the outcome and the result of international cooperation. Slovenia should continue and double its efforts to resolve the communication problems with the FIU and LEAs in a neighbouring jurisdiction, which seriously hamper the investigation and pursuit of ML with foreign underlying predicate offences.

17. Implement the newly adopted APMLFT effectively by developing relevant guidance and applying respective supervisory measures to ensure that obliged entities meet their obligations with respect to ascertaining beneficial owners and PEPs.

18. Slovenia should continue to implement its risk-based approach to supervision of the banking sector and improve the effectiveness of inspections in all other sectors by implementing a risk-based approach and targeted or thematic inspections when relevant. In this regard, the OMLP should urgently make use of its supervisory powers and ensure that it has the necessary resources.

19. Slovenia should take steps to improve the knowledge of supervisors regarding ML/FT risks, with specific emphasis on FT risk, and sharing of information between supervisors and the OMLP.

20. Slovenia should implement additional measures to allow supervisors to check criminal background and connections of individuals exercising control and management or supervisory board members of obliged entities, including obtaining information from other LEAs and tax authorities.

E. Effectiveness and Technical Compliance Ratings

Effectiveness Ratings

IO.1	IO.2	IO.3	IO.4	IO.5	IO.6	IO.7	IO.8	IO.9	IO.10	IO.11
Mod.	Sub.	Mod.	Mod.	Mod.	Mod.	Mod.	Mod.	Mod.	Mod.	Mod.

Technical Compliance Ratings

R.1	R.2	R.3	R.4	R.5	R.6	R.7	R.8	R.9	R.10
PC	LC	LC	LC	PC	PC	PC	PC	LC	LC
R.11	**R.12**	**R.13**	**R.14**	**R.15**	**R.16**	**R.17**	**R.18**	**R.19**	**R.20**
C	PC	PC	C	C	PC	LC	LC	LC	C
R.21	**R.22**	**R.23**	**R.24**	**R.25**	**R.26**	**R.27**	**R.28**	**R.29**	**R.30**
C	LC	LC	LC	LC	PC	C	PC	C	C
R.31	**R.32**	**R.33**	**R.34**	**R.35**	**R.36**	**R.37**	**R.38**	**R.39**	**R.40**
LC	PC	LC	C	C	LC	LC	LC	LC	LC

MUTUAL EVALUATION REPORT

Preface

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

2. This evaluation was based on the 2012 FATF Recommendations, and was prepared using the 2013 Methodology. The evaluation was based on information provided by Slovenia, and information obtained by the evaluation team during its on-site visit to Slovenia from 7 to 19 November 2016.

3. The evaluation was conducted by an assessment team consisting of:

Evaluators:

- Ms. Yulia Lafitskaya, Deputy Head of the International Legal Division of Legal Department, Federal Financial Monitoring Service, Russian Federation (legal evaluator)
- Mr. Tomislav Sertić, Head of Department for Inter-Institutional and International Relations, Anti-Money Laundering Office, Ministry of Finance, Croatia (legal evaluator)
- Mr. Nedko Krumov, Head of the International and Analytical Unit, FIU (FID-SANS) Financial Intelligence Directorate, State Agency for National Security, Bulgaria (law enforcement evaluator)
- Mr. Malkhaz Narindoshvili, Head of Legal, International Relations and Methodology Department, Financial Monitoring Service, Georgia (financial evaluator)
- Mr. Elhanan Harmor, Manager Licensees Supervision Unit, Investment Department, Securities Authority, Israel (financial evaluator)

MONEYVAL Secretariat:

- Ms. Veronika Mets, Administrator and assessment lead
- Mr. Lado Lalicic, Head of AML/CFT Monitoring, Typologies and Conference of the Parties to CETS no198 Unit
- Ms. Francesca Montagna, Administrator
- Ms. Anne van Es, Legal Assistant

4. The report was reviewed by the FATF Secretariat, Ms. Catherine Rabey, Advocate, Legislative Counsel Attorney General's Chamber, Guernsey and Mr. Giuseppe Lombardo, International Strategic Advisor – Financial Integrity.

5. Slovenia previously underwent a MONEYVAL Mutual Evaluation in 2010, conducted according to the 2004 FATF Methodology. The 2010 evaluation and 2013 follow-up report have been published and are available at http://www.coe.int/t/dghl/monitoring/moneyval/Countries/ Slovenia_en.asp. Slovenia's 2010 Mutual Evaluation concluded that the country was compliant with 14 Recommendations; largely compliant with 24; partially compliant with 10. Recommendation 34 ("Legal arrangements – beneficial owners") was assessed to be not applicable to Slovenia. Slovenia was placed under the regular follow-up process immediately after the adoption of its 4th round Mutual Evaluation Report, and was moved to biennial updates in April 2013.

CHAPTER 1. ML/FT RISKS AND CONTEXT

6. The Republic of Slovenia has a territory of 20,273 square km and a population of 2,064,241 (as of 1 July 2016). It is located at the crossroads of Central Europe and the Balkans and it borders with Italy, Austria, Hungary, and Croatia - all member states of the European Union (EU). Most of its territory is landlocked, with the exception of a short strip of coast line on the Adriatic Sea (46 km), which has three sea ports (Piran, Izola and Koper). The capital of Slovenia is Ljubljana with 288,179 inhabitants.

7. Slovenia is a parliamentary republic and legislative power is vested in the Parliament. The Parliament is bicameral, comprising the National Assembly which holds most of the legislative power (consisting of 90 deputies elected every four years) and the National Council, with limited advisory and control power (consisting of 40 appointed members). The executive power is exercised by the Government of Slovenia, headed by the Prime Minister and the Council of Ministers, who are elected by the National Assembly. The head of state is the President (directly elected), who holds a largely ceremonial position. Slovenia's legal system is based on civil law principles. Primary legislation is in the form of laws; secondary legislation is in the form of regulations. There are 211 municipalities in Slovenia. There is no official intermediate government layer between the municipalities and the Republic of Slovenia.

8. Slovenia joined the EU in 2004. In 2007, the country joined the EMU (Economic and Monetary Union), abandoning the tolar and introducing the Euro (EUR) as its official currency. The country is a member of numerous international organisations, including the United Nations (UN), the Council of Europe (COE), the Organisation for Security and Cooperation in Europe (OSCE), the World Trade Organisation (WTO), the European Bank for Reconstruction and Development (EBRD), the World Bank, the International Monetary Fund (IMF), the Organisation for Economic Co-operation and Development (OECD), and International Police (INTERPOL).

ML/FT Risks and Scoping of Higher-Risk Issues

Overview of ML/FT Risks

9. Slovenia is not a major international financial centre and does not have high domestic crime rates; nonetheless, its relatively stable and reliable financial sector may attract money launderers from the region. Its geographical position between the EU and the Balkans exposes Slovenia to external threats, including, in particular, drug trafficking. Furthermore, according to the authorities, there has been a surge in economic crime which can be attributed, inter alia, to the effects of the economic and financial crisis.

10. Slovenia finalised its work on a national risk assessment (NRA) in 2015 and adopted an updated version in 2016.

(a) ML threats

11. ML investigations are mostly linked to the investigation of criminal offences in the field of economic crime, and, to a lesser extent, to the areas of organised crime, corruption and general criminality. According to the NRA, the domestic economic crime offences which are deemed to pose the highest ML threat are abuse of position or trust in the performance of economic activities, tax evasion, business fraud and abuse of official position or official duties. Outside of the realm of economic crime, offences related to illicit drugs are deemed to pose the highest ML threat.

12. The offence **abuse of position or trust in the performance of economic activities** can qualify both instances of fraud and corruption in the private sector. According to the authorities, its enforcement is very challenging due to the economic and legal expertise and economic power of the perpetrators. Cases are often time-consuming and long-lasting and often require close cooperation between authorities, the involvement of financial experts and international cooperation. Whereas the share of this offence in total number of economic crime offences is low, the share of its damages

is estimated to be very high. In some uncovered cases, the amount of damages stemming from one offence was around or over 10 million EUR. Interviews on-site indicated that abuse in the medical and health-care industry are most prevalent and pose the highest ML threat.

13. The criminal offence of **tax evasion** has undergone various legal changes in recent years. Amended legislation in 2008 significantly extended the scope of criminalisation, resulting in an increased number of investigations and indictments. In 2012 however, the threshold for criminalisation was raised from 5,000 to 50,000 EUR of evaded taxes.[2] This legal change led to a decrease in the number of criminal complaints received for tax evasion, although the number of indictments remained relatively stable at around 100 per year. In 2015, the incrimination changed again: the act can now also be committed serial (with one or more acts related to one or more sorts of tax), and the total amount (sum) of concealed obligations in the period of 12 serial months at the most is now relevant. The authorities expect that this change will lead to an increase in the number of this criminal offence in the recent future. Cases of tax evasion mentioned in the NRA include legal entities committing VAT fraud (VAT carousels); the import of used vehicles from EU countries through letter-box companies; and other modalities through shell companies.

14. The most common form of **business fraud** is the non-payment of goods supplied or services performed, with criminal complaints often serving as means of putting pressure on debtors. Indictments have increased as a consequence of the deteriorated economic climate after 2008. According to the authorities, the crime often does not pose a significant ML threat as the damage frequently lies in unpaid obligations.

15. For **abuse of official position or official duties**, the authorities are of the opinion that many of the criminal complaints are ungrounded, made by persons who are not satisfied with decisions of competent authorities within official procedures. The authorities further determine the ML threat of other corruption related predicate offences ('acceptance of bribes' and 'unlawful acceptance of gifts') as low. They note that corruption at lower levels in Slovenia has been predominating, with low incidence rates involving low values of assets.

16. At the same time, the assessment team believes that reliance on official crime statistics on **corruption** may lead to a too brightly painted picture. Interviews on-site suggested that the low ML threat rating in the NRA for corruption may be due to the narrow choice of data to inform the rating and poor quality of statistics on the crime; and that corruption in Slovenia beyond lower levels may be more systemic. It appears to be a particular problem in the health sectors and in matters related to public procurement.[3] Decision-making within local governments (Slovenia has 211 municipalities) is also deemed to present a risk for corruptive activities.

17. The 2013 evaluation report of the Council of Europe Group of States against Corruption (GRECO) warned that true implementation of anticorruption legislation is yet to be secured and that there is a significant gap between legislation and practice.[4] The report also notes that there has been a strong public perception in Slovenia in recent years that corruption is increasing and constitutes a major national problem. Public confidence is particularly weak regarding politicians, with a widespread opinion that private interests decidedly affect the public sector. A 2012 report of Transparency International also warns of too close links between business and politics in the country.[5] In 2012, there were large street demonstrations calling for resignations of high-level public

---

[2] According to authorities, the reference period in which the threshold must be met depends on the type of tax – for property tax it is per year; for income for a natural person and for VAT it is per month.

[3] See also European Commission, *Business Attitudes Towards Corruption in the EU*, 2015, mentioning problems of lack of transparency in economic and commercial decision-making, unclear public tender processes and lack of transparency in public procurement as reported by potential investors and businesses in Slovenia.

[4] GRECO, *Fourth Evaluation Round: Corruption prevention in respect of members of parliament, judges and prosecutors – Evaluation of Slovenia*, 2014. See also European Commission, *EU Corruption Barometer*, 2014; and European Commission, *EU Anti-Corruption Report,* 2014.

[5] Transparency International*, National Integrity System Assessment on Slovenia*, 2012.

officials allegedly implicated in corruption.[6] In recent years, several cases of corruption of politicians and business tycoons were pursued in Slovenia, but with mixed success.[7]

18. The main ML threat from offences outside of the economic crime spectre stems from **illicit narcotics**. Slovenia is believed not to be a major drug producing country, but is a transit country for drug trafficking through both the Balkan route originating from the Middle East and the southern route through Africa.[8] The Government of Slovenia is aware of Slovenia's attractive geographic position for drug smugglers and pursues active counter-narcotics policies. The members of criminal associations active in this field are believed to be mostly Slovenian citizens with strong family and ethnical relations with West Balkan countries and citizens of countries of ex-Yugoslavia. The on-site interviews confirmed the ML risk posed by drug trafficking, mostly through usage of the Slovenian banking system as transit destination for funds.

19. With the exception of drug trafficking, an in-depth analysis of the external threat for ML posed by proceeds-generating offences committed abroad is missing in the NRA. Based on on-site impressions and review of open sources material, it appears that the most pertinent ML threat would arise from tax evasion offences committed in neighbourhood countries (such as Italy, whose NRA concluded that tax evasion is the single most important source of proceeds of crime),[9] and from organized crime in general, beyond drug trafficking, in particular linked to countries of the former Yugoslav Republic.

20. For example, one of the predicate offences for which the Slovenian Ministry of Justice (MJ) has received most requests for mutual legal assistance in the past years is **counterfeiting**.[10] A recent OECD/EUIPO report found that the propensity of Slovenia to export counterfeited goods to other countries has strongly increased up to a number that is quite high in comparison with other 'new' EU member state countries.[11]

21. Public sources consulted by the assessment team further indicate that Slovenia is a destination or transit country for victims of **human trafficking.** Main countries of origin of identified victims are Balkan and Eastern Europe countries and Slovenian citizens have been identified as perpetrators. Reports indicate that numbers of actual cases may be higher than identified due to insufficient law enforcement efforts, especially in relation to trafficking for purposes other than sexual exploitation.[12]

22. The assessment team also considered the fact that key illegal immigration routes to the EU run through the Western Balkans region.[13] The region is under major pressure since the refugee crisis that has emerged in Europe since the summer of 2015, which has not let Slovenia unaffected and which is believed to have fuelled **human smuggling** activities.[14] These developments also impact on the terrorist and terrorist financing threat that Slovenia is exposed to, as potential terrorists may

---

[6] OECD, *Anti-Bribery Convention Phase 3 evaluation of Slovenia*, 2014.
[7] Freedom House: *Nations in Transit – Slovenia*, 2015.
[8] Slovenian NRA; UNODC, *World Drug Report,* 2011; UNODC, *World Drug Repor*t 2015, and UNODC, *Afghan opiate trafficking via southern route*, 2015; Europol, EU Drug Markets Report, 2016.
[9] FATF, *AML/CFT Mutual Evaluation Report of Italy,* 2016.
[10] Slovenian NRA.
[11] OECD/EUIPO, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact,* 2016.
[12] GRETA, *Report concerning the implementation of the COE Convention on Action against Trafficking in Human Beings by Slovenia,* 2014; Eurostat, *Trafficking in human beings,* 2013; Trafficking in persons report - Slovenia, 2015.
[13] Europol, *EU Serious and Organised Crime Threat Assessment,* 2013; Frontex, *Western Balkan Route*.
[14] UNHCR, *New Balkan border restrictions untenable*, 2015; BBC News, *Migrant crisis: Slovenia moves to 'shut down' Balkans route*, 2016.

occasionally exploit the crisis and use the same routes and flows as refugees to travel to the countries where they plan attacks.[15]

23. The Western Balkans is also a transit region and a major source region of **illegal firearms** traded on the international weapons market. This may also impact on the risks of terrorism financing in the region. There are indications that weapons used in the recent terrorist attacks in Europe originate from the illegal weapon trade in the Balkans, pointing also at potential links between organized crime and terrorism.[16]

(b) ML/FT vulnerabilities

24. The **banking sector** accounts for the prevailing majority of the financial services industry in Slovenia and is deemed most vulnerable to ML. The cross-border transfer of funds, depositing and withdrawal of cash and real estate purchases frequently involving fictitious arrangements are perceived as the main challenges for banks. The large majority of STRs come from banking institutions. According to cases analysed by the OMLP, banks are used more frequently for ML than other financial and credit institutions.

25. One factor that is believed to contribute to vulnerability for the banking sector is poor corporate governance within the banks. The OECD noted in 2013 that "Slovenia is facing a severe banking crisis, driven by excessive risk taking, weak corporate governance of state-owned banks and insufficiently effective supervision tools" and linked the misallocation of credit to likely corrupt behaviour.[17] The authorities met on-site were of opinion that in recent years, the situation has improved.

26. According to the NRA, two other key deficiencies contributing to the vulnerability of the banking sector are the poor transparency of data on beneficial owners of foreign legal entities and lack of access to independent sources of information regarding natural persons as customers and their business.[18] A final key deficiency lies in insufficient action taken in cases of identified violations of AML/CFT obligations, with no sanctions imposed so far on banks.

27. **Other financial institutions** than banks are not deemed particularly vulnerable to ML. One of the companies providing payment services/transactions in Slovenia,[19] which previously only operated with banks as agents, has recently started to work with a chain of agents outside of the banking sector (kiosks). This can create higher ML risks.

28. The assessment team noted that the NRA rates several **DNFBP sectors** as medium vulnerable for ML. These vulnerabilities were further clarified during the on-site interviews. They include the misuse of trade with second-hand gold and craft materials, and the vulnerability of the gambling sector and the real estate sector to foreign criminality, mostly due to insufficient controls on the widespread use of cash. With regard to lawyers, fiduciary accounts from which lawyers can withdraw cash are believed to pose a ML risk. Furthermore, new emerging risks emerging from the

---

[15] Europol, *EU Terrorism Situation and Trend Report (TE-SAT* 2016). https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016

[16] Europol, *EU SOCTA,* 2013. The Slovenian Ministry of Defence recently hosted a regional South-eastern counterterrorism conference in 2016 on "Extremist Infiltration and Arms Smuggling in the Light of Migration Crisis in Europe", see www.mo.gov.si/en/media_room/conferences_and_congresses. See also various media sources.

[17] OECD, *Economic Survey of Slovenia,* 2013.

[18] With regard to the second of these deficiencies, one of the problems according to the NRA lies in the lack of access by banks to national databases on identity cards and driver's licences. The assessment team acknowledges that this can be seen as vulnerability. However the assessment team wishes to emphasize that this vulnerability may be common to many countries. Access to such databases is not a specific requirement under the FATF Recommendations and possibilities to eliminate this vulnerability may be trumped by data protection considerations. Therefore the assessment team considers that not too much particular weight should be given to this deficiency.

[19] The company is registered abroad and can operate in Slovenia through the EU passporting system.

potential abuse of virtual currencies (e.g. Bitcoin transactions) became apparent. The updated NRA also notes that a new risk has emerged in relation to illicit drug trade: sale of drugs via the internet.

(c) TF risks

29. Slovenia's geographic situation is relevant when considering the risks of terrorism and financing of terrorism that the country faces. Neighbouring countries in the Balkans region have seen a strong rise in terrorism risks in the aftermath of past regional conflicts, originating from separatist groups. Furthermore, some of these countries have already for many years noted the existence of NPOs in the region engaged in Islamist missionary work, with non-transparent funding from abroad. Recently, the wider region has experienced an increase in Islamist radicalisation and nationals joining the so-called Islamic State (ISIS) as foreign fighters in Syria and Iraq.

30. Slovenia itself reportedly has "little to no experience" with terrorism or the financing of terrorism. Slovenia has experienced one recent terrorist case (2015), in which an Italian citizen used a Slovenian post office to send letters with chemicals to Czech politicians. According to the NRA, information from the interministerial Working Group for Combating Terrorism, operating within the National Security Council, does not reveal any serious threats. Nevertheless, there are suspicions that 10 persons have left Slovenia to go to Syria or Iraq, and there is some recent information indicating activities in the field of training and recruitment for terrorist activities and promoting of radicalization.

31. Authorities and private sector representatives believe that developments with migrants transiting through or staying in the country have led to certain new risks faced by banks. Banks can take into account the cards of the applicant for international protection as appropriate identification document for customers who do not dispose of personal documents, but verifying the true identity of the customer with such cards remains a challenge.

Country's risk assessment

32. Slovenia completed its first ML/FT NRA in 2015 using the National Money Laundering and Terrorist Financing Risk Assessment Tool provided by the World Bank. The data used for this assessment mainly covered the 2010-2013 periods. In 2016, the authorities up-dated the NRA with the relevant data for 2014 and 2015. Another objective for updating the NRA was to obtain a better understanding of the FT risks. The updated NRA resulted in an action plan, endorsed by the Government in November 2016.

33. The World Bank methodology comprises three stages (initial workshop, desk review and final workshop), but due to budget restrictions only the first two stages were carried out. The initial workshop was held in Ljubljana, from April 16-18, 2014 with more than 60 participants from 40 different institutions, including the private sector. Participants were divided into seven working groups to assess the national threats and vulnerabilities and the sector-specific vulnerabilities. The main sources of information for the NRAs were different types of statistics and working group experts' opinions.

Scoping of Higher Risk Issues

34. The assessment team identified those areas which required an increased focus through an analysis of information provided by the Slovenian authorities, including the NRA, and by consulting various open sources, as discussed above.

35. **Predicate offences and financial investigations.** The assessment team met with the police and with the prosecution service to discuss the investigation and prosecution of the offences identified in the NRA as the most significant predicate offences to ML as well as the related ML offences. It also looked into how effectively the authorities cooperate at the domestic and at the international level on complex cases. Special attention was paid to law enforcement authorities' (LEAs) understanding of ML risks and whether and to what extent they pro-actively conduct parallel financial investigations. The functioning of specialized investigation teams, which are now provided for under the law, was also analysed by the assessment team.

36. **Corruption.** In the course of its meetings with LEAs and other authorities, including the Commission for the Prevention of Corruption, the evaluation team paid particular attention to corruption, both as a ML predicate offence and to assess its potential impact on the effectiveness of the ML/FT regime. During the interviews held with the obliged entities, the delegation also focused on how well risks regarding politically exposed persons, who are especially vulnerable to corruption, are assessed and managed.

37. **Organized crime and external threats.** Threats deriving from trans-border criminal activities and mitigating measures were considered in-depth in the course of the evaluation. Special attention was paid to the main typologies of external threats as understood by the authorities and the private sector, as this aspect was not duly taken into account in the NRA. These included, in particular, links with organized crime in the Western Balkans and other countries, the migration crisis and deficiencies in relation to cross-border cash control. The assessment team also looked into international cooperation sought and provided by Slovenia with other countries in pursuing organized crime and its proceeds.

38. **Temporary forfeiture and confiscation measures.** The results of the civil confiscation regime have been very modest and the effectiveness of the criminal confiscation regime is questionable. As a result, the evaluation team discussed at length with the authorities the functioning of both the criminal and civil regimes in place. In particular, it looked into the consistency between the criminal confiscation regime and the risk environment. During its interviews with LEAs and judicial authorities, the assessment team discussed the potential obstacles to imposing temporary seizure measures, the management of secured assets and the achievement of the recovery of assets.

39. **Financial institutions and DNFBPs.** The assessment team looked into how well domestic and cross-border ML and FT risks are understood and managed by financial institutions (in particular banks as they are deemed to be the most vulnerable) and DNFBPs. Cash transactions and internet transactions including through virtual currencies platforms were one of the main focus areas for the DNFBPs sector, and in particular for the real estate sector, the gambling sector and gold dealers. The assessment team also appraised how effectively supervisory bodies are responding to ML/FT risks and whether they are adequately resourced. The lack of targeted AML/CFT supervision for most DNFBPs, the inadequacy of corporate governance in the banking sector and the failure to impose fines for violations of AML/CFT obligations also received special attention.

40. **FT risks and implementation of targeted financial sanctions related to terrorism, FT and proliferation.** Slovenia's NRA contains only limited information on FT risks. As a result, the evaluation team verified whether Slovenia has assessed FT risks in line with current global and regional threats, including in relation to the NPO sector. Meetings were held with LEAs and intelligence authorities to appreciate their understanding of FTF risks and of the risk posed by NPOs which may be used to facilitate and fund the radicalization of individuals. The evaluation team also considered the NPO sector understands of their potential for being abused for FT purposes, and the extent to which authorities have conducted outreach to NPOs. In the interviews held with reporting entities, the assessment team paid particular attention to the level of awareness of their obligations regarding targeted financial sanctions related to terrorism, FT and proliferation.

41. The little transparency of data on beneficial ownership, in particular where foreign legal entities occur in ownership structures, represents ML vulnerability. Reported cases of tax evasion and ML often involve letter-box or shell companies which are "abandoned" after the commission of the criminal act. The assessment team discussed with the authorities the availability and reliability of data on basic and beneficial ownership, and the observed and expected effect of recent efforts to improve the prevention of the misuse of legal persons and arrangements for ML or FT. It also carefully assessed the level of understanding of the concept of beneficial ownership among obliged entities and the depth of checks on customers that they undertake.

Materiality

42. According to the World Bank, Slovenia is an upper income economy. Slovenia's 2015 Gross Domestic Product was 37.050 billion Euros (USD 42.775 billion). The economy is driven by the services sector (54.9% of GDP), industry (36.9%) and agriculture (8.2%). Foreign direct investment is an important component of the Slovenian economy. In 2013 it represented 3.8% of the GDP and was linked to trade, construction real estate and financial services.

43. The banking sector, which is comprised of 13 banks,[20] represents the biggest share of the financial sector. In 2013, the total assets of all banks and saving banks stood at 44.644 billion Euros, accounting for 126% of the GDP at the time. Seven of the banks are domestic, one of which holds subsidiaries abroad (in the Western Balkans). In most banks less than 3% of customers are classified as high-risk (including non-resident natural and legal persons, customers from high-risk jurisdictions, offshore corporate structures and certain businesses).

Structural Elements

44. The structural elements needed to ensure an effective AML/CFT system are generally present in Slovenia, including political and institutional stability, accountable institutions and the rule of law. The legislative framework is largely in line with international standards, with a few notable exceptions described in the TC Annex. AML/CFT policy-making and coordination is conducted through the Permanent Coordination Group for Prevention, Detection and Prosecution of Money Laundering and Terrorist Financing. The Group is composed of senior officials representing all the authorities involved in the prevention of ML/FT. The fight against economic crime including ML has been qualified as a high-level governmental priority in various national strategies (see further in Chapter 2).

Background and other Contextual Factors

45. Although levels of corruption in Slovenia are estimated to be relatively low on a global scale,[21] nonetheless, corruption could potentially have an impact on the effectiveness of the AML/CFT regime. Key institutions such as the specialized prosecutor's offices and police divisions for complex economic crime and the Commission for the Prevention of Corruption (CPC) have been established or strengthened in recent years in order to prevent and fight corruption. Publicly-available sources, however, suggest that these institutions require a considerable increase in resources and powers to effectively perform their role. There exists pronounced public scepticism towards the endeavours of the government to tackle corruption and the perception that prosecution services are not able to impose real punitive measures to efficiently deter corruption. In late 2013, the top leadership of the CPC resigned in protest against the lack of political support for more robust anti-corruption mechanisms.[22] It must also be noted that up until recently, there were no codes of ethics and committees responsible for ethics and integrity in place covering all prosecutors and judges.[23] GRECO called in its 2014 evaluation report of Slovenia for a reinforcement of the role of the governing bodies of the judiciary and prosecution services in developing integrity and managing corruption risks.[24]

46. The level of financial inclusion is very high: approximately 97% of the population holds a bank account.[25] A significant proportion of transactions carried out by non-bank FIs and their customers go through the banking system as progressivity of cash transfers is relatively low in Slovenia and

---

[20] Number of banks decreased to 12 due to acquisition in January 2017.
[21] Transparency International, Corruption Perceptions Index, 2015.
[22] GRECO, 2014; OECD, 2014.
[23] Slovenian NRA.
[24] GRECO, 2014.
[25] World Bank, *The Global Findex Database 2014 – Measuring Financial Inclusion around the World,* 2014.

cash payments for goods and services exceeding EUR 5,000 are prohibited.[26] Despite these characteristics, the use of cash is still identified as a risk factor for ML, which the evaluation team took into close consideration.

AML/CFT Strategy

47. ML/FT prevention is addressed in strategic documents which include a broader scope of prevention and detection of (economic) criminal offences. In line with these strategic documents, Slovenia has introduced a number of measures in recent years to strengthen its fight against economic crime (see Chapter 2).

48. From an institutional point of view, the OMLP is considered as the main actor in AML/CFT policy making and in formulating the relevant strategic documents. According to the authorities, in 2017 the OMLP should adopt its new internal Strategy for Money Laundering and Terrorism Financing Prevention.

49. Slovenia has not taken a coordinated approach to improve its national AML/CFT policies based on the results of the first NRA. The up-dated version of the NRA was used to trigger the elaboration of a national Action Plan setting out measures to mitigate the identified ML threats and vulnerabilities. No actions were proposed regarding FT, as the authorities consider such risk as low and well mitigated (see Chapter 2). The new APMLFT was adopted to implement the fourth anti money laundering Directive of the EU (Directive (EU) 2015/849).[27]

50. With regard to FT, a working group for the fight against terrorism at the strategic level operates under the National Security Council since October 2001.

Legal framework

51. Act on the Prevention of Money Laundering and Financing of Terrorism (APMLFT) stipulates measures, competent authorities and procedures for detecting and preventing money laundering and terrorist financing and governs the inspection of the implementation of its provisions. Money laundering (ML) is criminalized under Art. 245(1) of the Criminal Code (CC) and financing of terrorism (FT) is criminalized under Art. 109(1) CC. As for targeted financial sanctions (TFS), Slovenia implements the relevant UN resolutions mainly through the EU mechanisms. The legal basis for TFS is set out in the Act relating to Restrictive Measures Introduced or Implemented in Compliance with Legal Instruments and Decisions adopted within International Organisations (ARM).

Institutional Framework

52. The institutional framework for the development and implementation of Slovenia's AML/CFT policies includes the following agencies:

53. **The Permanent Coordination Group for Prevention, Detection and Prosecution of Money Laundering and Terrorist Financing** (Group) was created in 2012; the Group has a coordination role in streamlining AML/CFT policies, cooperating in the field of AML/CFT in international bodies and preparing actions plans on the basis of the MONEYVAL's recommendations. Chaired by the director of OMLP, the Group is composed of the representative of the OMLP, the MoJ, the Ministry of Foreign Affairs (MFA), Ministry of Finance (MoF) and the Police. The representatives of the BoS, the

---

[26] World Bank, 2014. OECD, 2014c., page 22, http://www.oecd.org/eco/surveys/Slovenia-2015-overview.pdf . In addition, according to Slovenian authorities total volume of cash transactions in 2015 was about 6,143 billion EUR, which represents 16 % of GDP in 2015 (38,570 billion of EUR).

[27] DIRECTIVE (EU) 2015/849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

State Prosecutor's Office and of the Supreme Court are also invited to the Group's meetings. If needed, other state authorities and supervisory authorities such as the Securities Market Agency (SMA), the Insurance Supervision Agency (ISA), the Market Inspectorate of Republic of Slovenia (MIRS), and the Financial Administration of the Republic of Slovenia (FARS), the Bar Association, and the Chamber of Notaries can also be invited to the Group's meetings.

54. **The Office for Money Laundering Prevention (OMLP) of Slovenia** is a structural part of the Ministry of Finance of Slovenia. It is an autonomous and operationally independent body carrying out FIU functions. More specifically, it is authorized to:

- Receive and request suspicious activity reports (SARs), cash transactions reports as well as other documents, disseminate the results of its work to the competent authorities;
- Propose to the competent authorities changes and amendments to regulations concerning AML/CFT;
- Conduct strategic analysis based on typologies, draw up the list of indicators for the identification of high risk customers and transactions and publish at least once a year statistical data on ML and FT;
- Supervise obliged entities and conduct off-site and on-site inspections (since the adoption of a new APMLFT Law in 2016);
- Submit designation proposals in the context of TFS;
- Temporarily suspend a transaction in case of suspicion of ML/FT;
- Coordinate the Interdepartmental Group for the execution of the NRA;
- The OMLP can request and provide information in a timely and effective manner from/to other FIUs spontaneously and upon request.

55. **The Bank of Slovenia (BoS)** has extensive powers to licence, register and supervise banks, MVTS and exchange offices. To perform its supervisory functions, the BoS performs different types of examinations and determines bank's AML/CFT profiles. Furthermore, Bank of Slovenia participates in the preparation of AML/CFT legislation, actively cooperates with the banking industry and takes part in international committees (MONEYVAL, EU AML committee etc.).

56. **The Slovenian Police Authority** is an independent agency within the Ministry of Interior. The Slovene Police is the main LEA in charge of investigating predicate offences, ML and FT. The coordination and analysis of, as well as, oversight and supervision over the work of the Police in the field of ML is entrusted to the Financial Crime and Money Laundering Section (FCMLS) which is structurally part of the Economic Crime Division, Criminal Police Directorate, General Police Directorate. As regards FT investigations, there is no specialized unit for FT investigation. At the same time, the Counterterrorism and Extreme Violence Section (CEVS), which a part of the Organised Crime Division of the Criminal Police Directorate, is responsible for supervising counter-terrorism investigations.

57. **The Ministry of Foreign Affairs of Slovenia (MFA)** is the chair of the Sanctions Coordination Group (SCG) and contributes to the coordination of the implementation of restrictive measures. It is responsible for the official flow of information regarding sanctions imposed by the UN and EU. For instance, the MFA of Slovenia is the competent authority for submitting listing proposals to the UN Security Council and to the CP 931 Working Party within the Council at the EU level. Furthermore, natural and legal persons are required to inform the MFA of accounts and amounts frozen under UN or EU legislation.

58. **The State Prosecutor's Office of Slovenia** is under the authority of the Ministry of Justice and its organisational structure consists of:

- the Office of the State Prosecutor General of the Republic of Slovenia (State Prosecutor's Office) is the highest-ranking prosecutor's office in the country having with jurisdiction over the entire

territory of Slovenia. The Expert Information Centre (EIC) is an internal organisational unit within the Office of the State Prosecutor General of the Republic of Slovenia which coordinates cooperation on confiscation. It keeps a central register of all proposals and orders related to confiscation and provide expert assistance to the State Prosecutors on the matter;

- **the Specialised State Prosecutor's Office (SSPO)**, was established in 2011 to prosecute serious criminal activities in the areas of organised traditional and economic crime, terrorism, corruption and other criminal activities requiring detection and prosecution by specially organised and trained state prosecutors. The jurisdiction of the SSPO also extends to the entire territory of the Republic of Slovenia;

- 11 district State Prosecutor's Offices, which have jurisdiction in the territory of a District Court of general jurisdiction and Local Courts pertaining to the territory of this District Court.

59. **The Ministry of Finance of Slovenia** (MoF) is the authority which has competence over decisions in relation to the authorisation of access to funds or other assets in accordance with R.6 and R.7 (targeted financial sanctions). The Ministry also closely cooperates with the MFA who chairs the SCG. Upon request from the MFA the MoF would provide support to the MFA on the legal issues in connection with financial services. The MoF is also giving non-binding legal advice to the business (banks) on the legal questions connected to AML/CTF.

60. **The Ministry of Justice of Slovenia (MoJ)** is the central authority in the provision of mutual legal assistance (MLA). Although, according to the CPC, MLA requests are to be sent via diplomatic channels, in practice, MLA requests are submitted directly through the MoJ which also ensures their timely prioritization and execution. Furthermore, the MoJ keeps statistics on the type and the number of requests made, received, processed, granted or refused (with countries outside of the EU).

61. **The Financial Administration of Slovenia (FARS)** enforces the physical cross-border reporting of currency and BNIs of value which is above of maximum threshold of 10.000 Euros.

62. **The Commission for the Prevention of Corruption (CPC)** is an independent administrative body with a mandate to prevent and investigate corruption. Although the CPC is not a LEA, it is empowered to accomplish a wide range of executive and supervisory tasks. The CPC can also request the OMLP to open a case.

63. **The Slovenian Intelligence and Security Agency (SOVA),** is the central civilian intelligence and security service responsible for the protection of national security. SOVA, as well as its military counterpart, the Intelligence Security Service, acquire and analyse information as part of FT and counter-terrorism investigations. SOVA has also the power to request the OMLP to collect information on a particular case.

64. **Supervisory Authorities:** APMLFT designates the institutions which carry out AML/CFT supervision of financial institutions and DNFBPs including the: BoS, SMA, Insurance Supervision Agency (ISA), Office of the Republic of Slovenia for Gaming Supervision (ORSGS), Tax Administration of the Republic of Slovenia (TARS), MIRS, Agency for Public Oversight of Auditing (APOA) and Slovenian Institute of Auditors (SIA), Bar Association of Slovenia, and Chamber of Notaries of Slovenia. An analysis of the functions and remits of the supervisory authorities can be found under R.26-28.

Financial sector and DNFBPs

65. Slovenia is not a regional or international financial centre. It has a relatively small financial sector compared to neighbouring states such as Italy, Austria, Hungary and Croatia.

66. The Slovenian financial system is dominated by banks that hold 70% of the total financial sector assets. In recent years, the Slovenian banking sector has been characterized by recapitalization and

consolidation. There are 13 banks[28] operating in Slovenia, including seven domestic and six foreign. The parent banks of all subsidiary banks and branches are headquartered in the EU member states (Austria, Italy, and France).

67. Only one Slovenian bank has subsidiaries outside of Slovenia; these are mainly located in the Balkan region. With regard to the type of banking services, Slovene banks do not offer sophisticated products to their customers. As concerns the types of customers, the large majority of clients are natural persons (91%). The share of non-residents in the overall customer base is estimated at 2.2% among natural persons and 0.8% among legal entities with comparable turnover figures.

68. As concerns the insurance sector, there are currently 15 life insurance and non-life insurance companies in Slovenia. The insurance market is not highly-developed and in 2014 the country ranked 13th among the EU member states regarding the share of the total insurance premiums in GDP. The non-life insurance sector dominates life in terms of gross premiums written making up about 73% of premiums.

69. The securities sector in Slovenia is relatively small compared to the banking and insurance sectors. At present, 5 brokerage companies[29] and 9 asset management companies[30] are operating in the country. Over the last 5 years, Slovenia's securities sector has been shrinking due to the global and domestic financial crisis, political crisis and stalling reforms. As for the clients, it should be emphasized that the number of foreign customers, especially high-risk clients is low.

70. Other financial institutions in Slovenia include currency exchange operators (23), payment and electronic money institutions (3), pawnshops (7), lenders and credit intermediaries other than banks and savings banks (68) and leasing companies (22).

Table 1: **Overview of financial institutions in Slovenia**

Name of the sector	Number
Banks	13
Insurance companies	15
Payment institutions	3
Agents of foreign Payment Institution from MS	5
E-money institutions **Distributors of foreign electronic money institution from MS**	1 1
Securities (brokerage companies)	3
Asset Management companies	9
Currency Exchange operators	23
Pawnshops	7
Lenders and credit intermediaries other than banks and savings banks	68
Investment pension funds	3
Leasing companies	22

[28] Since January 2017 there are 12 banks operating in Slovenia. Two banks (one of them was foreign subsidiary) were merged in January 2017.
[29] Since January 2017 there are 3 brokerage companies.
[30] Since January 2017 there are 8 asset management companies.

71. The DNFBP sector in Slovenia comprises casinos (including internet casinos), real estate businesses, lawyers, notaries, and auditors, dealers in precious metals and stones and providers of accounting services. According to authorities there are no trusts and company service providers (TCSPs) in Slovenia.[31] Some parts of the DNFBP sector such as loan agencies, tax advisors, real estate agents and traders in precious metals are not properly supervised. There is also a lack of information regarding the size of the sector and the number of entities.

Table 2: **Overview of DNFBPs in Slovenia**

Name of the sector	Number of Entities	Competent authority
Casinos, gaming halls, providers of classic games of chance, internet casinos	6 casinos. 30 gambling halls, 2 providers of classic games of chance, 3 internet gambling providers.	FARS
Trading in own real estate, intermediation in real estate	260 (legal persons and sole traders)	FARS and Market Inspectorate for real estate agents
Lawyers	1200	Bar Association
Notaries	92	Chamber of Notaries
Auditors	Certified auditors: 190 Audit firms: 54	Agency for the Public Oversight Over Auditing
Dealers in Precious stones and metals and goldsmiths	2 registered dealers, 112 registered goldsmiths and jewellers (but registration is not mandatory)	Market Inspectorate
Providers of Accounting services	more than 4.500	Chamber of Accounting Services

Preventive measures

72. The cornerstone of the Slovenian AML/CFT regime is the newly adopted Act on the Prevention of Money Laundering and the Financing of Terrorism (APMLFT) which replaces the APMLFT that was in force since 2008.

73. The preventive framework in Slovenia is broadly in line with the requirements of the FATF standards. At the same time, mitigation of ML/FT risks is hindered by some technical deficiencies as well as effectiveness gaps. For instance, several DNFBP sectors including registered dealers in precious metals and stones and scrap gold traders are not subject to AML/CFT supervision. There are also gaps in the existing legal framework regarding wire transfers as the inclusion of beneficiary information is not mandatory. Other factors which negatively affect the preventive framework include relatively low understanding of FT risks by banks, insufficient appreciation of ML/FT risks by DNFBPs, limited awareness of beneficial ownership requirements and the unawareness among the DNFBPs of the existence of higher-risk countries identified by the FATF.

74. On the other hand, the implementation of preventive measures is strengthened by supervisory guidelines and red-flag indicators developed by the OMLP and other supervisory bodies for the reporting entities under their supervision.

[31] However from public resources it could be seen that there are businesses which provide company services.

Legal persons and arrangements

75. On 30 September 2016, Slovenia had 206,152 registered entities in the Slovenian Business Register. These statistics also include several professionals (natural persons) such as attorneys, doctors and artists, and public bodies such as courts and local communities. The overwhelming majority of business entities take the form of limited liabilities companies and sole proprietors. Other corporate entities are unlimited companies, limited partnerships, and public limited companies (also often referred to as 'joint-stock companies', economic interest groupings and cooperatives. Economic interest groupings can be formed by two or more companies to facilitate and promote the gainful activity of its members in an auxiliary manner. The purpose of a cooperative is to facilitate economic benefits and develop economic and social activities of its members. They may engage in any activity in which a company may engage and must register these activities under the same rules as companies. In addition, there are legal persons that are generally used for other purposes, such as trade unions, religious communities, associations for sports, culture or humanitarian work, and private institutes.

76. Slovenia ranks 49th among 190 economies in the World Bank's Ease of Doing Business rankings.[32] Interviews on-site indicated that processes for setting up companies have been significantly streamlined in recent years. The practice of 'one-stop-shops' to facilitate the set-up of a company without having to involve a notary (this applies to all types of companies with the exception of public limited companies) has contributed to this development.

77. Around 17% of limited liability companies are foreign-owned; 7 % of unlimited companies and 6% of limited partnerships. Only 1 public limited company is foreign-owned. The statistics are however based on member and/or founder address being outside of Republic of Slovenia and may not represent actual foreign ownership in all instances.

78. Table 3: **Overview of legal persons in Slovenia**

Type of legal person	Number
Sole proprietor	86,095
Limited liability company	70,245
Unlimited company	737
Public limited company	705
Limited partnership	379
Limited partnerships with share capital	2
Limited liability cooperative	325
Non-liability cooperative	111
Economic interest grouping	148
Association	23,290
Institute	3,243
Foundation	292

Source: OMLP based on Slovenian Business Register

79. Around 31,500 NPOs operate in Slovenia. The main types of non-profit organisations are associations (74%), institutes (10%), religious communities (4%) and foundations (1%). They are subject to registration requirements and obtain legal personality upon registration. Associations and

[32] http://www.doingbusiness.org/rankings.

institutes are established by multiple natural or legal persons for the purpose of pursuing their joint interests and activities in the fields of education, science, culture, sports, health, social protection etc. Foundations are assets linked to a specific purpose, which may have a public benefit or a charitable purpose, or both. The Law on Foundations explicitly prohibits foundations to the benefit of specific individuals – a foundation must define its beneficiaries otherwise in its founding act (e.g. victims of domestic violence). There is no possibility to establish a foundation for private interests (e.g. for descendants of a family).

80. Slovenian legislation does not regulate the establishment or operation of trusts and legal arrangements. Slovenia is not a Party to the Hague Convention on Laws Applicable to Trusts and their Recognition. At the same time there are no provisions precluding trusts or similar legal arrangements established under foreign law from conducting their activities through the Slovenian financial system, and there are no prohibitions for persons under the jurisdiction of Slovenia to act as trustees of such foreign legal arrangements. The evaluation team found no examples of appointments of Slovenians as trustees during the interviews. The evaluation team did find examples of legal arrangements which featured in the ownership structures of some clients of banks.

81. The evaluation team identified a Slovene type of legal arrangement that falls under IO.5/R.25. It concerns UCITS mutual investment funds which represent assets in a mutual fund owned by the holders of investment coupons and separate from the assets of the company managing the fund. All investment funds in Slovenia are currently formed in this way (rather than established as an investment company which is a legal entity) and the total value of their assets is circa 2,41 billion (November 2016). The manager of the mutual fund is responsible for compliance with the requirements of the APMLFT on obliged entities (Art. 4 (1) point 6 APMLFT).

Supervisory arrangements

82. Table 4 describes supervisory arrangements which came into force during the on-site with APMLFT. Sectors and services are listed following the Article 4 (obliged entities) of APMLFT. The licencing/registration regime is in place with other relevant legislation.

Table 4: **Supervision of FIs and DNFBPs**

Name of the sector/services	**Licensing/Registration**	**AML/CFT Supervisor**	**Relevant legislation**
FIs			
Banks[33]	Licensing	BoS, OMLP and SMA[34]	Banking Act (2015) and APMLFT
Insurance companies[35]	Licensing	ISA and OMLP	Insurance Act (2016) and APMLFT
Payment institutions	Licensing	BoS and OMLP	Payment Services and Systems Act (2009) and APMLFT
E-money institutions Distributors of foreign electronic money[36]	Licensing	BoS and OMLP	Payment Services and Systems Act (2009) and APMLFT

[33] Article 4 (1) 1. and 2. of APMLFT

[34] Article 151 (2) of APMLFT. SMA supervises banks only in the field of performing investment services and business (and not the bank as a whole).

[35] Article 4 (1) 14. of APMLFT

Post office if it provides services of money transfer (payments and disbursements) through a postal money order	Licensing[37]	OMLP	Postal Services Act and APMLFT
Securities (brokerage companies)	Licensing	SMA and OMLP	Financial Instruments Market Act (ZTFI) and APMLFT
Investment funds that sell their own units in the Slovenia	Licencing	SMA and OMLP	Investment Funds and Management Companies Act and APMLFT
Management companies and managers[38]	Licensing	SMA and OMLP	Investment Funds and Management Companies Act and APMLFT
Branches of an investment company, management company or manager[39]	Licencing	SMA and OMLP	Investment Funds and Management Companies Act and APMLFT
Managers of mutual pension funds	Licensing for Pension Company and authorization for a member of the Management Board of Pension Company	BoS, ISA, SMA and OMLP	Pension and Disability Insurance Act (IPDI-2) and APMLFT
Bridging facility governing bridging insurance for professional and top athletes	Licensing not required	ISA, SMA and OMLP	The Bridging Insurance of Professional and Top Athletes Act and APMLFT
Founders and managers of pension companies	Authorization for a member of the Management Board of Pension Company	ISA, BoS, SMA and OMLP	Pension and Disability Insurance Act (IPDI-2) – Articles 333 and 337; Insurance Act and APMLFT
Currency Exchange offices	Registration	BoS and OMLP	Foreign Exchange Act and APMLFT
Pawnshops	No requirement for licensing or registration	MIRS and OMLP	APMLFT
Lenders and credit	Licensing	MIRS and OMLP	Consumer Credit Act and

[36] Article 4 (1) 15. of APMLFT
[37] Licence given by the Agency for Communication Networks and Services of the Republic of Slovenia)
[38] Article 4 (1) 7. of APMLFT
[39] Article 4 (1) 9. and Article 4 (1) 10. of APMLFT

intermediaries other than banks and savings banks[40]			APMLFT
Financial leasing	Licensing	MIRS and OMLP	Banking Act, Consumer Credit Act and APMLFT
Issuing and managing other means of payment[41]	No requirement for licensing or registration	OMLP	APMLFT
Issuing and managing virtual currencies, including the service of exchanging virtual currencies to standard currencies and vice versa	No requirement for licensing or registration	BoS and OMLP	APMLFT
Issuing of guarantees and other commitments	No requirement for licensing or registration	OMLP	APMLFT
Portfolio management services for third parties and related advice, and investment management for the Slovenia in accordance with the law, governing the Slovenian Sovereign Holding	No requirement for licensing or registration	OMLP	APMLFT
Safe custody services	No requirement for licensing or registration	OMLP	APMLFT
Brokerage in concluding credit and loan business[42]	No requirement for licensing or registration	MIRS and OMLP	APMLFT
Insurance agency services for the purpose of concluding life insurance contracts	Licensing	ISA and OMLP	Insurance Act and APMLFT
Trust and Company	No requirement for	OMLP	APMLFT

[40] Article 4 (1) 20. a) of APMLFT
[41] Article 4 (1) 20. c) of APMLFT
[42] Article 4 (1) 20. h) of APMLFT

service Providers	licensing or registration		
DNFBPs			
Organisers and concessionaires organising games of chance	Licensing	FARS and OMPL	Gaming Act and APMLFT
Notaries	Licensing	Chamber of notaries	Notaries Act and APMLFT
Auditing firms and independent auditors	Licensing	The Agency for Public Oversight of Auditing and the Slovenian Institute of Auditors	Auditing Act (2008) and APMLFT
Real estate agents[43]	Registration	Market inspectorate and OMLP	the Real Estate Mass Valuation Act and OMLP
Trade in precious metals and precious stones or products made from these materials	No requirement for licensing or registration	Market Inspectorate and OMLP	APMLFT
Trade in works of art	No requirement for licensing or registration	OMLP	APMLFT
Organisation and execution of auctions	No requirement for licensing or registration	OMLP	APMLFT
Lawyers and law firms	Licensing	Bar Association	Lawyers Rules (2008) and APMLFT
Tax advisors	No requirement for licensing or registration	OMLP	APMLFT
Accountants	No requirement for licensing or registration	OMLP	APMLFT

83. In addition, the FARS, in accordance with its competencies, shall exercise supervision of the implementation of prohibitions against the acceptance of payments for goods and performed services in cash in an amount exceeding €5,000 by legal entities and natural persons.

International Cooperation

84. Slovenia's geostrategic position and its status as a transit country for drug trafficking and other forms of organized crime activity raises the overall ML risk level and the need for international cooperation in this field. Most ML-related cooperation is undertaken with neighbouring countries, both from the EU and with non EU States from former Yugoslavia.

[43] Article 4 (1) 20. r) of APMLFT

85. The Ministry of Justice (MoJ) is the central authority which handles international requests pursuant to a number of bilateral and multilateral treaties on which Slovenia relies for providing and requesting MLA and extradition. Domestic courts decide on the execution of requests. The OMLP is the central authority for the Council of Europe's 1990 and 2005 Conventions for Laundering, Search, Seizure and Confiscation.

86. As a member state of the EU, Slovenia is actively engaged in judicial cooperation at the EU level. The Slovenian Act on Cooperation in Criminal Matters with the EU Member States (ACCMEU) regulates direct communication between judicial authorities of EU member states, mutual recognition in criminal matters, surrender under the European arrest warrant, transfer of proceedings, transfer of the execution of sentences and cooperation with EU entities such as Eurojust and Europol. The increasing use of direct communication with the EU has resulted in the decrease in the amount of incoming and outgoing requests for MLA and extradition dealt with by central authorities.

87. The OPML, Police, and Tax Authorities cooperate with their foreign counterparts through bilateral and multilateral Memorandum of Understandings (MOUs), treaties, the principle of reciprocity, and other cooperation mechanisms such as Interpol and the Egmont Group of Financial Intelligence Units.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

1. The authorities have partially succeeded in identifying, assessing, and understanding ML risks. This is primarily done through the first NRA, completed in 2015, and its update, completed in 2016. The NRAs show some weaknesses, in particular related to sources of information and their further use.

2. While the OMLP and the LEAs show a satisfactory level of understanding of all country-relevant ML threats and vulnerabilities, the supervisory institutions do not have such a broad understanding and are either mostly focused on their own sector risks (FIs supervisors) or generally unaware (DNFBP supervisors). One of the reasons for such incongruity could be that, after the elaboration of the threat and vulnerability assessments in the NRA project, there has been no final coordination of understanding and steps to be taken to mitigate the identified risks.

3. The NRAs contain a very limited analysis of FT threats and vulnerabilities. The overall understanding of FT risks varies between stakeholders, but is at a satisfactory level among the LEAs, OMLP and security service. A national strategy for combating terrorism and FT is yet to be adopted.

4. The obliged entities' understanding of ML risks is uneven. In the financial sector, it is mostly based on own analysis and group-level policies rather than on NRA results. The DNFBPs have limited knowledge about sector specific ML/FT risks and are not vigilant and insufficiently trained regarding general country ML/FT risks. The awareness of FT risks is generally low across all sectors although higher among a number of banks.

5. OMLP is considered to be the key authority in the development and implementation of AML/CFT policies and activities. Additionally, there are numerous interagency working groups, committees and mechanisms to facilitate policy-making and operational coordination. However, these have not yet led to sufficient risk-sensitive allocation of resources, and mitigation policies and national co-operation and co-ordination of AML/CFT policies and activities could be strengthened.

6. Slovenia has not taken any specific steps to improve its national AML/CFT policies after the adoption of the first NRA. The Action Plan elaborated after the updated NRA appears to be rather general and some of the prescribed mitigation activities are described ambiguously. However, in

some areas (mainly with regard to the AML/CFT activities of BoS and OMLP) a risk-sensitive approach to mitigating risk had been used already prior to the NRA project.

Recommended Actions

Slovenia should:

1. Undertake a more detailed assessment of ML/FT risks that broadens the types of information used in the process (i.e. typologies, case studies and comparable statistics), ensures the participation of all relevant stakeholders and covers areas that were overlooked in the first and updated NRAs. Special attention and resources should be dedicated to ensuring that the assessments of threats and vulnerabilities result in a joint understanding of ML/FT risks among stakeholders.

2. Ensure that the AML/CFT Action Plan includes clear objectives and actions to be taken by each of the competent authorities consistent with the ML/FT risks, and specifies their intended outcomes in order to allow for proper monitoring of the effectiveness of their implementation.

3. Strengthen the use of existing national coordination and cooperation platforms to monitor implementation of AML, CFT and CPF policies and activities, including in the supervisory field, and to propose improvements accordingly.

4. Improve the understanding and vigilance of the private sector through more targeted communication and sharing of comprehensive information on ML and FT risks identified at the national level and on the need for implementation of policies and activities to combat PF.

5. Ensure that CDD exemptions and enhanced measures for higher risk scenarios and simplified measures for lower risk scenarios are based on a proper assessment of ML/FT risks.

88. The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The recommendations relevant for the assessment of effectiveness under this section are R.1-2.

Immediate Outcome 1 (Risk, Policy and Coordination)

Country's understanding of its ML/FT risks

89. Slovenia completed its first ML/FT NRA in 2015. Before conducting the NRA, Slovenian authorities undertook other initiatives to explore and mitigate the country's economic crime threats by developing general strategies against (economic) crime. These earlier initiatives have, however, not been used to fully understand and capture the ML/FT component. The assessment team, in evaluating Slovenia's understanding of its ML/FT risks, focussed predominantly on authorities' understanding of ML/FT risks as reflected in the outcomes of the NRA and took also into consideration the general understanding and initiatives by relevant stakeholders.

90. Slovenia's first ML/FT NRA covered data mainly for the period 2010-2013. Its updated NRA (in 2016) used data for 2014 and 2015. The chosen methodology was the World Bank ML/FT methodology elaborated for global purposes. The government was acquainted with the updated version of the NRA and adopted the accompanying Action Plan during the period of MONEYVAL's on-site visit. All relevant governmental authorities and some participants of the reporting entities were included in the preparation of the first NRA. The update of the NRA was predominantly done by the governmental authorities.

91. The inclusion of the private sector in the NRA process provides more diversity to the risk identification and assessment. However, it appears that some financial institutions, including the banks and most of the DNFBP sectors were not consulted in-depth during the NRA process but only requested to provide statistics on their sector. The knowledge that they can have as gatekeepers on high-risk situations, products and clients was therefore insufficiently exploited. The NRAs also do not cover properly stakeholders in those areas where there are gaps in existing supervisory activities, mainly with regard to money remittance services outside the banking sector, certain real estate agents, financial and tax advisors and accountants.

92. Both NRAs include an assessment of threats and vulnerabilities mostly with regard to ML. The evaluation team notes that the updated NRA contains limited elaborations as compared to the first version, especially with regard to the DNFBP sector, where statistics were often lacking and most parts were directly extracted from the previous document. On the positive side it shall be noted that Slovenia is the first MONEYVAL country to update its NRA.

93. The main sources of information for the ML threat assessment in the NRAs were relevant expertise and statistics provided by the Police and the Prosecutor's Office on criminal complaints and indictments for proceeds generating crimes. The statistics proved not to be easily comparable as they use different units of measurement (i.e. per case or per suspect). The participants of the Threat Working Group (the Police and Prosecutor's Office) paid due attention to the challenge to deduce conclusions from the sometimes inconsistent statistics. Nevertheless, the threat assessment could have benefited further from the inclusion of case studies, information on on-going intelligence work and investigations, and statistics on convictions. This way, more insight could have been obtained in the most recent trends in criminal activities and in consistency of law enforcement efforts and results with the country's ML risk profile.

94. Open source information was used in the analytical process, but this appears to have substantially informed conclusions of the NRAs only as far as transnational organised drug crime is concerned. In general, consideration of the impact of foreign criminality on the ML threat in Slovenia was limited. Except for drug trafficking, the participants of the Threat Working Group were convinced that organised or economic criminality transiting through Slovenia, or committed in neighbouring countries, does not materially influence the ML threat level for Slovenia. They believe that these crimes often do not involve Slovene nationals and did not find indications that the individuals involved are laundering money in Slovenia. The evaluation team considers, however, that the public sources described in Chapter 1 and interviews with the private sector and authorities on-site in some cases certainly suggest otherwise. The impact of external threats should therefore have warranted more in-depth consideration in the NRA process.

95. The national and sectorial vulnerabilities in the NRAs were assessed by using supervisory and other available statistics, an assessment of the current legislation and the findings of some international documents in the AML/CFT area. Typologies derived from case studies were also used. The latter was a rather rare practice and applied without a clear methodology or model governing on which occasion and basis cases were to be selected, analysed and used to inform conclusions.

96. The representatives responsible for the ML threat assessment within the NRAs reported that they strengthened those parts of the World Bank methodology which were deemed most useful for Slovenia. Most of the representatives responsible for the vulnerability assessments of the NRAs on the other hand appeared to have strictly followed the provided global tool, even where they sometimes found that this did not allow them to sufficiently take the country's specificities into consideration. In addition to its participation in the NRA process, the BoS has undertaken its own risk assessment for the banking sector in which some of the findings of the NRA regarding banking sector vulnerabilities were questioned. The BoS was of the opinion that the chosen methodology for the NRA did not allow it to select all the right issues for the banking sector.

97. After the elaboration of the threat and vulnerability modules of the NRAs, no final coordination exercise has been undertaken in order to integrate the findings on identified threats and vulnerabilities into a joint understanding of risks. The on-site interviews indicated that the NRA process lacked adequate financial and political support for such a final identification of risks. The final stage of the World Bank methodology – a workshop to integrate findings – was not held. Requests from authorities to nevertheless organise a meeting to discuss the outcomes in-depth were allegedly declined.

98. The consequences of the omission of this final stage became apparent during on-site interviews. Among several stakeholders, understanding of risks appears to be based more on subjective perceptions than on objective analysis. The level of understanding of national ML threats and

vulnerabilities varies significantly among the competent governmental authorities. While the OMLP and the LEAs demonstrate a satisfactory level of understanding of all country-relevant threats and vulnerabilities, the supervisory institutions, with the exception of the banking sector, are focused mainly on their own sector risks. They sometimes even appear to have a less complete understanding of the sectorial risks than the supervised entities. Whilst there is logic in supervisors focusing their efforts on sectorial risks, the assessment team is of the opinion that supervisory authorities should be aware of generally recognised country risks as well. This will allow them to have a wider view on the ML/FT threats and vulnerabilities and give them the ability to proactively search for high-risk situations during their supervisory actions.

99. In the Slovenian NRAs, some major ML risks highlighted by the private sector were not sufficiently analysed; and understanding about these risks among institutions shown to be uneven. This is particularly pertinent with regard to: possible abuse of virtual currencies; the vulnerability of the gambling sector to foreign criminality; the use of cash, including in cross-border situations; the vulnerability of the real estate sector for integration of foreign criminal assets; the misuse of dealers of precious metals, mainly with regard to trade with second-hand gold and craft materials; tax evasion crimes involving foreign elements; and risks associated with financial institutions licensed abroad but operating also in Slovenia. Some of these risks are recognised and understood by the LEAs, OMLP and some of the reporting entities, albeit in a non-systematic way which does not allow for a coordinated mitigating approach.

100. Corruption involving middle and high-level officials presents a ML risk in Slovenia. This was mentioned by a number of representatives from the public and private sector and assessed in the NRAs. Whilst the use of domestic and foreign legal entities appears to be a usual practice for laundering the proceeds of such criminal activities, this is not elaborated as a vulnerable area in the NRAs. In addition, the NRAs do not contain an analysis on the level of threat which Slovenia faces with regard to foreign bribery, given Slovenia's strong economic links to countries with high risks of corruption. Nevertheless, the LEAs are well aware of the threat presented by the highly-fragmented municipal divisions in Slovenia and some other economic particularities of the country (e.g. medical and pharmaceutical sectors). The Slovenian authorities are also well aware of ML risks related to the abuse of position or trust in the performance of economic activities, which is an important private sector corruption-related offence. The BoS was also aware of an increased risk that the proceeds of corruption could be laundered at subsidiaries of Slovenian banks in higher-risk countries and has taken coordinated action with the host supervisors to mitigate these risks.

101. The insufficient level of training and specialisation of judges with regard to ML cases (see IO. 7), was mentioned as an area of higher vulnerability during interviews because it may impede the development of ML jurisprudence. Although the potential impact of jurisprudence on the effectiveness of AML efforts is not mentioned explicitly in the NRA, the NRA does recognise that due consideration should be given to further judicial reorganisation in order to improve the courts' ability to decide on complex cases of organised and economic crime.

102. The NRAs do not contain an in-depth analysis of FT risks. In the first NRA, the FT threats were only assessed from the perspective of the number of STRs reported to the OMLP and vulnerabilities were seen only from the perspective of the size of the NPO sector. In the updated NRA, the FT threat has been analysed from a preventive perspective, taking into consideration the institutional, policy and operational level structures in place in the country and domestic and international cooperation and information flows.

103. During the on-site visit, it became apparent that the FT threats and vulnerabilities are nonetheless consistently understood among the competent LEAs, the security service and the OMLP. The direct threat for Slovenia is generally assessed as low but authorities acknowledge that recent developments have increased the risks and warrant high vigilance. According to their understanding, the most significant emerging threats are the potential for: local NPOs to support international fundamentalist religious terrorism; the exploitation by terrorists of recent migration movements and support of Slovenian citizens travelling to conflict zones abroad to join foreign terrorist groups.,

The authorities consider the geographical location of the country in the Western Balkans, money flows in cash and money flows through payment institutions as Slovenia's main vulnerabilities. In the last five years, none of the investigations carried out with regard to potential terrorist activities uncovered evidence of FT activities. The authorities stated that both possible domestic and foreign terrorists and foreign fighters under scrutiny were self-financed or received donations from NPOs. No direct intention to finance a terrorist criminal offence could, however, be proven, as required by Article 109 of the CC. The deficiencies of the FT offence should be taken into consideration when considering the results of the investigations carried out (see under IO.9 and R.5). It must further be noted that, whilst the LEAs, OMLP and security service demonstrated sufficient levels of knowledge, the supervisory institutions were generally unaware with regard to the particular FT vulnerabilities and threats faced by Slovenia.

National Policies to Address Identified ML/FT Risks

104. At policy level, the Slovenian institutions mostly rely on activities performed within the context of joint committees, working groups and national strategies, adopted or formed by Parliament or the government. Slovenian authorities had national policies and platforms, including certain risk-sensitive features, even before the elaboration of the first NRA. To some extent the areas of ML and FT have been covered in high-level strategic documents of recent years which include a broader scope of combating criminal offences. Very recently, pursuant to the update of the NRA, the government adopted an AML/CFT Action Plan, which however suffers from a number of deficiencies (see further below).

105. The main strategic documents in the economic crime area are the Resolution on National Plan on Prevention and Combating of Crime for the period 2012 – 2016, adopted by Parliament in 2012, and the Strategy of Managing Economic Crime adopted by the Government in 2012. The purposes of the Resolution were: evaluation of the relevant situation in the field of economic crime; and proposal of activities for better cooperation and coordination of competent authorities in the field of the fight against pecuniary crime, economic crime and corruption, with special attention to the "follow-the-money" principle, seizure and confiscation. The Strategy aims to establish and ensure the effective investigation of criminal offences against the economy, corruption and prosecution of perpetrators together with the seizure and confiscation of illegally derived assets.

106. For both the Resolution against Crime and the Strategy against Economic Crime, an interdepartmental working group has been established by governmental decision which promotes and monitors the implementation of the programmes and tasks. At least once a year, both groups report on their implementation to the Government of Slovenia (which sends the report to Parliament in the case of the Resolution).

107. In line with the strategic documents, Slovenia has introduced a number of measures in recent years to strengthen its fight against economic crime. Examples of this are the decisions in 2010/2011 to establish the National Bureau of Investigation within the Police and to establish a Specialised Prosecutor's Office to better investigate and prosecute complex economic and organized crime, and to allocate additional resources to them in 2014. Some of the measures taken by the General Police Directorate based on the Strategy are detailed in Box 1. The OMLP has also been given additional resources since 2014 (two employees in the supervision and prevention department and two in the suspicious transactions department) as a result of the government's objective to combat serious economic crime.

Box 1: Police Action Plan to implement the Strategy of Managing Economic Crime

Pursuant to the Strategy of Managing Economic Crime in the Republic of Slovenia, the Director General of the Police has adopted an Action plan to implement the strategy's basic and strategic goals. An example of points in the Police Action Plan concerns the improvement of material and technical equipment of economic crime investigators. This activity is based on the Strategy's overarching basic goal: efficient and effective detection, investigation and prosecution of criminal acts and their perpetrators in the areas of economic crime and corruption, and the seizure of

proceeds of crime.

In line with the Action Plan, the IT and Telecommunications Office of the General Police Directorate has upgraded the police database on financial investigations data. The upgraded database has been in use since November 2013 and has been additionally upgraded with data collected under the Forfeiture of Assets of Illegal Origin Act (FAIOA) – the law governing civil confiscation. The database supports the operational activities of criminal investigators and enables supervision and creation of statistical data on financial investigations under both the Criminal Procedure Act and FAIOA. In addition, the most outdated economic crime investigators' computers have been replaced. A computer application for easier and more efficient monitoring of the confiscation of illegal assets, and training of criminal investigators on use of the application, have also been developed.

108. The authorities are currently preparing a new Resolution on Prevention and Combating of Crime for 2017-2022. They have advised that, as was the case for the 2012-2016 Resolution, objectives will be set widely and no specific AML/CFT measures will be included.

109. With regard to FT, it can be noted that terrorist criminal offences in general are included as a threat that needs priority action in the 2012-2016 Resolution against Crime and in the National Security Strategy of the Republic of Slovenia (last version adopted by Parliament in 2010). Based on the National Security Strategy, a joint strategic working group for the fight against terrorism has operated under the National Security Council since October 2001. It is composed of high-level representatives of intelligence, law enforcement and defence agencies and includes the FARS and OMLP. The group regularly issues a classified terrorism threat assessment which can include information on FT on a case-by-case basis.

110. The 2010 National Security Strategy foresees that a national strategy on prevention and combating terrorism would be adopted, but this has yet to happen. A draft form of such a strategy, which includes the prevention of FT as one of the key measures on preventing terrorism, has been prepared and is under consideration. It is unclear whether this strategy will determine risk-sensitive policies and activities (periodic risk assessments and risk-based allocation of resources) as a key focus in combating FT. Furthermore, it is not expected that this strategy will also have a preventive approach to invest much-needed efforts in increasing the level of knowledge within the private sector to detect FT (see core issue 1.6 below), given that it is drafted by the Police.

111. In 2012, a Permanent Coordination Group for Prevention, Detection and Prosecution of Money Laundering and Terrorist Financing was established. The main goals of the Group are exchanging of information, domestic and foreign cooperation and coordination, preparation of action plans, training and education. However, it appears that a lack of dedicated resources has so far hampered the ability of the relevant authorities to develop targeted national AML/CFT policies within the Group.

112. Slovenia has not coordinated its approach to improving its national AML/CFT policies based on the results of the first NRA.[44] The updated NRA was, however, used as a starting point for the development of a national Action Plan which sets out measures to mitigate the identified ML/FT threats and vulnerabilities. The OMLP has developed the Action Plan in consultation with the institutions that participated in the NRA process. Since the Action Plan was elaborated only very

[44] However, the updated NRA and Action Plan include one example where the authorities have already started to take action on identified deficiencies in the first NRA. Namely, in the field of asset freezing and confiscation, the Ministry of Justice has proposed amendments to the CPC to extend time-limits for provisional securing and has undertaken an analysis of storage and management of the temporarily secured and seized assets. Parallel with the NRA and updated NRA processes, the Slovene authorities have been working on the elaboration of the new APMLFT, which was adopted during the on-site visit.

shortly before the evaluation visit, the evaluation team could not yet draw any conclusions on its implementation.

113. During interviews, some participants of the NRA project (mainly with regard to the securities sector) expressed disagreement with the deficiencies and actions in the Action Plan. In the opinion of the evaluation team, the adopted Action Plan is rather general. Some of the prescribed mitigation activities are ambiguous. Further steps will need to be taken to decide in more detail how the mitigating measures shall be applied in practice. The authorities would also benefit from more specific articulation of the expected results of mitigation measures and the outcome measurements (i.e. to what extent is this measure expected to decrease the ML/FT risk and how shall this be measured?). This way, the authorities will be better positioned to monitor if chosen mitigation activities are effective and to what extent they should be applied or changed in the future.

114. The Action plan does not include any particular FT related measures as the authorities consider the FT risk to be low and well mitigated. The evaluation team, however, became aware of specific FT threats and vulnerabilities that would deserve further attention. Crucial examples are the gaps in the FT offence which hamper effective law enforcement action (see R.5 and IO.9) and the lack of awareness among reporting entities on FT (see core issue 1.7 below and IO.4 and IO.9).

115. The Action Plan formulates certain measures which will influence the adjustment of supervisory priorities. The strategic documents mentioned above do not appear to have had an effect on supervisory policies and their risk-based application, as they focused mainly on repressive law enforcement action.

116. From an institutional point of view, the OMLP is considered as the main participant in the above-mentioned policy-making platforms and formulation of strategic documents as far as AML/CFT is concerned. The OMLP has adopted its new internal Strategy for Money Laundering and Terrorism Financing Prevention (2015-2020). The OMLP demonstrated a sufficient level of understanding of the nationally identified risks and the need for a better risk-based allocation of its resources in the future (see paragraph 116 below).

Exemptions, enhanced and simplified measures

117. Article 9 of the new APMLFT foresees that the findings of the NRA report will improve national AML/CFT regulation, in particular by defining sectors or activities where the obliged persons must apply stricter CDD and other measures. At the time of the on-site visit, no clear policies in that regard based on the NRA had yet been developed. In general, it appears that the new AML/CFT legislation in Slovenia on exemptions, enhanced and simplified CDD measures are not based on NRA risk scenarios, but are the result of the transposition of the EU Directive 2015/849.

118. Given the recent adoption of the NRAs and the very recent entry into force of the new APMLFT, the evaluation team could not assess whether the implementation of exemptions, enhanced and simplified measures in Slovenia is consistent with the NRA results. The envisaged processes for allowing exemptions in the APMLFT (for e-money providers, organisers and concessionaires organising games of chance outside of casinos and gaming halls, legal entities, sole proprietors and individuals that perform certain financial activities individually and only occasionally) do appear to be based on risk. They will only be granted in cases of proven low risk following a risk assessment, in limited and justified circumstances, and for a particular type of institution or activity. See more on exemptions, enhanced and simplified measures under R.1 and R.10.

Objectives and activities of competent authorities

119. Although some initiatives have been undertaken, the evaluation team is of the view that Slovenia should focus more strongly on ensuring that objectives and programmes of competent authorities are consistent with nationally recognised policies and risks.

120. All supervisory authorities' objectives on management and executional levels are primarily focused on the prudential side of supervision. The BoS is the only authority which has introduced a

specialised structure for AML/CFT supervision. BoS is also the only institution which uses an AML/CFT risk-based supervisory methodology. ISA and SMA and all DNFBP supervisors do not consider ML/FT risks in setting objectives, planning activities and allocating resources. To date, most of the on-site inspections have been carried out on rule-based principles and have been more technically orientated by checking the existence of measures rather than assessing their sensitivity to identified risks and their risk-mitigating effects.

121. The LEAs are focused on their current operational priorities, which include economic predicate crime investigations and to some extent ML. As mentioned earlier, the Slovenian LEAs benefit from the strategic documents mentioned above. However, none of them allocate resources on an ML/FT risk-sensitive base. Furthermore, potential ML is not pursued in predicate offence criminal cases or parallel financial investigations to an extent that is commensurate with the ML risks (see further IO.s 6 and 7).

122. As outlined in the Introduction and earlier in this chapter, the evaluation team considers corruption more of a threat for ML than recognised in the NRA or acknowledged by some of the government authorities interviewed. The establishment and gradual increase in powers of the Commission for the Prevention of Corruption, an autonomous and independent state authority, is therefore an activity worthy of attention. The Commission cannot be considered as a LEA in pre-trial and criminal proceedings, but it has certain executive, supervisory and investigative powers (which are not dependent on any authorisation). The Commission has a significant role in elaborating strategic documents and policies to help the government and other competent authorities in understanding and preventing corruption. At the operational level, the Commission has been used mainly as a source for initiation of investigations, for reporting of suspicious transactions to the OMLP and for determination of corruption profiles.

123. The OMLP adapts its policies based on internal strategic analyses and the NRA. The post-NRA Action Plan recognises the OMLP as the institution which shall most often react to the identified ML/FT risks. The OMLP has been allocating resources on a risk-sensitive basis prior to the NRA, especially in prioritisation of STR analysis. Nonetheless, this is done on a case-by-case basis (by disposition of the Head of the Analytical Department or the Director of OMLP) without using any special methodology or other consistent approach. In general, the OMLP is proactive in sharing its observations on emerging risks with the private sector. Some examples of warnings issued in recent years relate to observed usage of fake ID cards, ID cards issued to migrants, import and exchange of certain suspicious currencies, Bitcoin transactions, and transactions with certain high-risk countries.

National Coordination and Cooperation

124. Most of the policy making initiatives described above that touch upon ML/FT in Slovenia are coordinated and adopted at the high political level. There are a number of other mechanisms in place that support cooperation and coordination between relevant authorities on ML/FT issues, including information exchange, such as memoranda of understanding.

125. Daily cooperation between the OMLP and the supervisory authorities in the financial sector is a sufficient tool for fit and proper assessments made during the market entry procedures. Furthermore, it is clear from interviews that the OMLP serves as a single point of contact for AML/CFT relevant issues for other governmental agencies. Supervisory and other authorities know how to find the OMLP in case of questions about interpretation of relevant legislation. The market associations and chambers are valuable partners in the AML/CFT coordination process with the private sector in Slovenia. The main focus of their work is provision of guidelines and communication channels with the respective supervisors, usually on their own initiative. It appears, however, that there is a lack of regular and systematic sharing of information among supervisors as well as between supervisory authorities and the OMLP, such as on typologies and trends or planning of inspections. This lack of cooperation hampers the collective understanding required to effectively identify and mitigate ML/FT risks.

126. Some confusion over division of supervisory competences became apparent during interviews (i.e. MVTS providers operating outside of banks and investment services provided by banks, see IO.3). The evaluation team further considers that the cooperation between the OMLP and the BoS related to training (especially in the FT area) and the NRA process are areas for further improvement, especially in light of the importance of banking sector ML risks which demand strong mutual understanding of risks and mitigating action. Furthermore, the evaluation team considers that not all relevant stakeholders' opinions were sufficiently taken into consideration in the elaboration of the post-NRA Action Plan.

127. The evaluation team was informed that, as foreseen under the new APMLFT (Articles 7 and 155), a working group will be created to unite all supervisors, including the OMLP which will have new supervisory powers.

128. There are good communication channels and exchanges of information between the OMLP and the competent LEAs and intelligence services. The OMLP receives annual feedback from the Prosecutor's Office and feedback from the Police, primarily statistical data. The OMLP is used to gather additional information on ML/FT related intelligence cases and parallel financial investigations by the Police and security service, especially with regard to banking information, ATM withdrawals, identification of authorised persons and international cooperation. The OMLP has also taken part in almost every investigative team operating since 2012 for civil confiscation proceedings, and can take part in special investigative teams for complex economic crimes, which can also involve tax officers (see IO.s 7 and 8).

129. As described under core issue 1.2, a working group for the fight against terrorism operates at strategic level under the National Security Council. At operational level, there are regular contacts between law enforcement and intelligence (OMLP, civil intelligence, military intelligence) on signals for terrorist and FT activity. The evaluation team had the impression on-site that relevant information, including from foreign counterparts and in case of possible matches with international FT sanctions lists, flows regularly between these stakeholders.

130. Slovenia has elaborated coordination policies with regard to combating proliferation of weapons of mass destruction and its financing through the permanent Sanctions Coordination Group (SCG) chaired by the Ministry of Foreign Affairs. Nevertheless, the resources available to members of the group to dedicate themselves to the topic seem insufficient, and subsequently the level of vigilance of the institutions is negatively affected (see IO.11).

131. It can be concluded that Slovenia has already taken important steps to establish national coordination and cooperation mechanisms and platforms to monitor the implementation of AML, CFT and CPF policies and measures. Nonetheless, the evaluation team is of the view that further improvements are needed in their policy-setting and practical use to make them more effective tools in the domestic AML/CFT system. In particular, the formulation of more targeted AML/CFT policies within the context of the general fight against economic crime and terrorism would be desirable to guide the work of authorities, and more attention should be paid to a risk-sensitive allocation of resources.

Private Sector's Awareness of Risks

132. All supervisors were involved in the NRA process. Nevertheless, those who are mainly responsible for DNFBP supervision did not demonstrate a good level of understanding of the threats and vulnerabilities identified during that process (except for the OMLP). The evaluation team believes that this has resulted in a deficient dialogue with some reporting entities and uneven understanding of the major ML/FT risks among supervisors. The evaluation team further became aware that communication between the OMLP and the BoS has, on some occasions, been shown to be ineffective (see previous section above and under IO.3). This can additionally hamper the awareness-rising process on ML/FT risks in the banking sector.

133.The OMLP has reportedly communicated the need for risk-based allocation of resources to reporting entities via the most recent training. However, no guidance has been provided to reporting entities so far to point out the importance of organising AML/CFT activities on a risk-sensitive basis. The new APMLFT contains obligations in that respect (Art. 13-15 in particular), but, due to the recent entry into force of the law, its effect was not yet discernible throughout the private sector.

134. At the time of the on-site visit, a summary of the first NRA report had been published on the website of the OMLP. The first NRA report was disseminated to participants of all NRA working groups, which included private sector representatives. Some reporting entities interviewed on-site participated in the first NRA workshop (banks, casinos, securities market representatives). Some other sectors were represented by their member associations (notaries, lawyers, accountants). None of them were invited to actively participate in the process to up-date the NRA in 2016. At the time of the on-site visit, no decision had been taken yet on publication, or distribution, of (a summary of) the updated version.[45]

135. Except for the banking and securities supervisors, which took some actions to share the NRA results with their supervised entities, the evaluation team was not informed of any activities undertaken by the other competent authorities to actively communicate the results of the NRA to obliged entities. The level of awareness regarding the results of the NRA among representatives of most reporting entities was low. Except for representatives of the private sector who participated themselves in the NRA process, most were largely unaware of its results. Assessors also noted that the level of understanding among representatives of the private sector of vulnerabilities and threats identified at the national level is variable.[46] Non-bank FIs and DNFBPs' understanding is rather low compared to the understanding by the banking sector. DNFBPs are also not vigilant about AML/CFT risks and insufficiently trained.

136. Interviews with all reporting entities demonstrated a lack of understanding in relation to potential FT indicators. This could result from an absence of active awareness-raising activities by the competent public institutions. Many reported not having mechanisms in place to detect possible FT or PF activities and not having received any instructions on this issue from competent authorities. The banking sector demonstrated a relatively higher, but still limited, level of understanding of FT risks which is primarily based on information received from their groups headquartered outside Slovenia and the awareness-raising policies of the BoS. The lack of understanding among reporting entities could ultimately hamper the understanding of risks among authorities, as indicators may not be brought to their attention.

Overall conclusions on Immediate Outcome 1

137. Strategies and activities to set priorities and coordinate policies in the fight against economic crime and terrorism and to facilitate cooperation between competent authorities pre-date the NRA. The evaluation team welcomes the fact that Slovenia has recently undertaken its first NRA involving all relevant stakeholders, in which ML threats and national-level and sectorial vulnerabilities were considered. The efforts invested by the national authorities in assessing, understanding and, to some extent, mitigating the existing ML/FT risks are notable. Nevertheless, the full potential of the NRA process to develop a full and common understanding of the most pertinent ML/FT risks and to identify the most appropriate mitigating measures has not yet been exploited. This was visible also from the sometimes differing levels of understanding of national risks among the competent authorities.

---

[45] After the on-site visit, the OMLP published the NRA report and updated NRA report on its website. The underlying materials that form part of the methodology were not published. www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/NRA_objava.pdf, www.uppd.gov.si/fileadmin/uppd.gov.si/pageuploads/dokumenti/NOT_posodobitev_2014_2015.pdf

[46] The extent to which FIs and DNFBPs use their understanding of the countrywide ML/TF risks to apply the necessary risk mitigating measures is discussed under IO.4 (core issue 4.2).

138.Slovenia should invest further efforts in improving the communication with the private sector to increase its level of understanding of the national risks. This is needed especially with regard to FT, on which information provision on risks is currently inadequate. Furthermore, Slovenia has not fully exploited the existing possibilities for coordination of policies offered by the various mechanisms in place and has not yet made risk-based allocation of resources one of the pillars of its AML/CFT regime.

139.The Action Plan adopted in November 2016 appears to be good starting point for further improvement of measures to mitigate ML/FT risks. Nonetheless, the shortcomings explained in this chapter, coupled with deficiencies in the NRA process that it is based on, currently make it an insufficient tool for adequately improving the effectiveness of the regime.

140. **Overall, Slovenia has achieved a moderate level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

1. Financial intelligence in Slovenia derives from a range of information collected by the OMLP and law enforcement agencies (LEAs). These institutions have access, directly or indirectly, to a broad range of financial, commercial, real estate, tax and customs information.

2. The statistics and information provided during the on-site have revealed a number of issues which directly influence the effective use of financial intelligence in ML and predicate offences related investigations. This primarily concerns the standard of proof set by the jurisprudence which the OMLP and LEAs perceive as considerably high and the respective laws (e.g. for tax crimes). This has been the principal reason for the relatively low number of ML disclosures compared to the number of ML criminal investigations.

3. The OMLP systematically uses and analyses the reports on suspicious and cash transactions (STRs/CTRs) received from the reporting entities. The vast majority of STRs is submitted by banks and is considered to be of a good quality. The reporting from other sectors (i.e. non-banking financial institutions and DNFBPs) has had a limited influence on the quality of financial intelligence given the low number of STRs which have been submitted.

4. The OMLP also performs strategic analysis and is considered to be one of the main policy making institutions in Slovenia. The police are more focused on the operational and investigative actions and so far have not made any specific ML/FT strategic analyses.

5. LEAs have initiated a limited number of FT investigations and it appears that financial intelligence is more often used to pursue terrorism cases. The Slovenian Intelligence and Security Agency (SISA) has reported that in all such cases OMLP powers in gathering financial data have been used.

6. Communication between the OMLP and law enforcement authorities is efficient and the level of feedback received is satisfactory. The deficiencies identified in relation to the effective use of financial intelligence does not stem from lack of capacity or cooperation between LEAs and the OMLP but are primarily related to the legal and other contextual factors applicable in Slovenia.

7. Financial intelligence is held securely, thus the risk of confidentiality breaches is low. Information is stored and exchanged in line with the requirements set by the Law on Classified Information which has been properly applied by the OMLP.

Immediate Outcome 7

1. Certain Law Enforcement Authorities are adequately trained in conducting financial investigations and in pursuing ML. However, overall, the fight against ML activity is not fully prioritised. The

number of ML investigation has steadily risen. Nonetheless, there is still a significant mismatch between the number of ML investigations and the number of investigations and convictions of proceeds generating predicate offences.

2. ML investigations and prosecutions reflect to some extent the risks that the country faces. ML investigations are mostly linked to the investigation of criminal offences in the field of economic crime (domestic tax evasion, abuse of position or trust in business activity, fraud/business fraud). On the other hand, Slovenia's risk profile would warrant a higher number of ML investigations related to serious crimes. Convictions also reflect to some extent Slovenia's risk profile.

3. In the period under review, the authorities have made progress in securing ML convictions, including in relation to third-party ML as well as autonomous ML. Practitioners, however, are faced with a number of obstacles in prosecuting and adjudicating ML cases, including: uncertainty as to the evidentiary requirements in proving ML and the underlying predicate offence; judges' and prosecutors' insufficient expertise on financial forensics/crimes, as well as insufficient administrative personnel; and in relation to ML cases in which the underlying predicate crime has been committed in a neighbouring jurisdiction.

4. Sanctions in the CC are commensurate with other profit-generating crimes. Custodial sentences which have been imposed, however, are at the lower end of the "sanctioning" scale and the fines imposed on legal persons have been too lenient. Furthermore, when a petition for extraordinary legal remedies is submitted, the statute of limitation is considered too short for certain complex cases.

5. A number of criminal justice measures are applied in cases where an ML investigation is pursued but it is not possible to secure an ML conviction.

Immediate Outcome 8

1. Asset recovery has been identified as one of the key policy objectives within the general policy documents on combating proceeds generating crime. However, this has not been sufficiently pursued in practice.

2. There are no legal limits as to the type and nature of property that can be subject to confiscation. In practice authorities face difficulties to recover types of assets other than funds.

3. Confiscation of criminal proceeds is mandatory under the CC; it includes confiscation of proceeds and instrumentalities obtained through the crime for which the perpetrator has been convicted. Extended confiscation cannot be ordered in the context of criminal proceedings, except in relation to property that a criminal organisation (or of its member) has acquired or has at its disposal.

4. A civil confiscation regime has been introduced in 2011 enabling authorities to confiscate property in civil proceedings. It has so far produced very limited results as almost all civil confiscation decisions were pending before the Constitutional Court of human rights/constitutional infringements at the time of the onsite visit.

5. Although the confiscation regime has a comprehensive legal basis, some technical, institutional and practical issues hinder its effectiveness. This primarily concerns the insufficient timeframe to gather evidence and obtain a court order to secure the assets; the absence of specialised institutions responsible for the management of assets; the low level of execution of confiscation decisions; the insufficient use of asset sharing mechanisms; and lack of comprehensive statistics.

Recommended Actions

Slovenia should:

Immediate Outcome 6

1. Encourage LEAs to use financial intelligence more actively when clear indicators on the specific predicate offence are missing. In this regard, further guidance and training should be developed for

prosecutors and LEAs to enhance the use of financial intelligence when pursuing ML in cases where information on the specific predicate crime is missing.

3. Provide guidelines on how to improve cooperation between the Police, the OMLP the Financial Administration and prosecutors in gathering evidence on ML and in tracing assets deriving from tax related criminal offences as a predicate crime.

4. The OMLP and LEAs should be proactive in seeking information held by DNFBPs and BO information collected by FIs/DNFBPs which can be used as a basis for financial intelligence in the pre-investigative and investigative phases.

5. Increase the number of specialised staff performing ML/FT financial intelligence analysis in the OMLP and the Criminal Police Directorate.

6. The OMLP should develop an internal analytical methodology to process and analyse STRs.

Immediate Outcome 7

1. Parallel financial investigations, alongside or in the context of the criminal investigation, should be systematically organised, particularly in serious and complex proceed-generating cases.

2. The authorities should be more proactive in investigating and prosecuting ML related to serious crime, in line with Slovenia's risk profile.

3. Clarity should be shed on the judgments issued in 2014 and 2015 by the Supreme Court, including on the interpretation given on evidential thresholds for establishing the underlying predicate criminality. Training to prosecutors and judges on such evidential thresholds should be provided and prosecutors should present the judiciary with more cases in which the underlying offence(s) is not unequivocally established.

4. Both the prosecution and judicial authorities should be provided with the required expertise on financial crimes and financial forensics. Additional administrative staff should also be deployed in the judiciary.

5. Slovenia should take steps to enhance the dissuasiveness of sentences and lengthen the statute of limitations which applies when a petition for an extraordinary legal remedy has been submitted.

Immediate Outcome 8

1. Establish a legal and institutional framework which ensures the effective and systematic management of confiscated assets.

2. Ensure the collection of reliable and detailed statistics on confiscation (including with a break down by type of ML predicate offence and cross border movement of cash) so that the effectiveness of asset recovery and the consistency of the efforts with the country's risk profile can be assessed.

3. Continue to pursue confiscation as a policy objective and ensure the provision of permanent training and specific guidelines (for prosecutors) so that parallel financial investigations are carried out systematically along with the criminal investigations of a predicate crime(s).

4. Ensure that controls of cross-border transportation of currency include the proper identification and investigation of ML/FT suspicions in line with the country's risk profile.

5. Make effective use of existing asset sharing mechanisms with foreign jurisdictions.

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

Immediate Outcome 6 (Financial intelligence ML/FT)

Use of financial intelligence and other information

142. Financial intelligence in Slovenia derives from a range of information collected by LEAs (mainly the Police) and the OMLP.

143.The OMLP has access, directly or indirectly, to a broad range of financial, commercial, real estate, tax and customs information (Table: Databases to which the OMLP has direct online access).

Table 5: **Databases to which the OMLP has direct online access**

Database holder	Available information	Searching criteria
OMLP	STRs Database	Name/Surname
OMLP	CTRs Database	Name/Surname
OMLP	International requests	Name/Surname
OMLP	Notifications to Police	Name/Surname
OMLP	Cross border in Cash	Name/Surname
OMLP	Wire transfers to high-risk countries	Name/Surname
AJPES	Company register	Company name/address/tax number/UIN
AJPES	Declared income of legal persons (3 years)	Name/Surname
AJPES	Bank Accounts of legal persons, with history *(no proxies information available)*	Name/BAN
AJPES	Bank Accounts of natural persons with history	Name+Surname+TAX NUMBER /BAN
Commercial database	Directors, members of board, founders, share holders	Name/Surname
Police	Criminal records (before prosecutor/court decision)	Name + Surname + DOB
Police	Wanted persons	Name + Surname + DOB
Tax Administration	Declared income and taxes paid (natural and legal persons)	TAX NUMBER
Tax Administration	Inspections concluded/on going	TAX NUMBER
Ministry of Interior	Register of natural persons (name, address, personal documents, vehicle)	Name + Surname/DOB/address
Ministry of Interior	Register of Personal documents	Type + Number
Ministry of Interior	Register of Tax numbers	TAX NUMBER
Ministry for Infrastructure	Vehicle register	Vehicle reg number
Ministry for Infrastructure	Vessel register	Vessel reg number

The Surveying and Mapping Authority of the Republic of Slovenia	Land/Building ownership records-natural persons	Name + Surname + TAX NUMBER
The Surveying and Mapping Authority of the Republic of Slovenia	Land/Building ownership records-legal persons	Name + UIN
The Surveying and Mapping Authority of the Republic of Slovenia	Land/Building data	Cadastral number of real estate
Court Cadastrial Register	Real estate register	Cadastrial number of real estate
Health Insurance Institute of Slovenia	Social security information (employment)	Name + Surname + PIC + DOB
Central Securities Clearing Corporation	Present securities ownership	Name/Surname + DOB
Central Securities Clearing Corporation	Register of issued securities	Name of Issuer

144. The OMLP makes regular and timely use of these databases and the information contained therein. This concerns all STRs and other cases opened upon STRs or information received from the reporting entities and the international counterparts. Currently the OMLP is in the process of developing an internal data-managing software system with a protected Internet portal which will receive STRs. The authorities have reported that this system will enable automatic checks of all information available in the afore-listed databases. Nonetheless, within the timeframe of the on-site visit this system was not fully operational, thus its effectiveness cannot be assessed.

145.Once an STR is received, the OMLP may request additional information from the reporting entities. Such requests can be submitted to all FIs or DNFBPs regardless of whether the entity has submitted an STR. These requests are submitted in hard copies. Table 6 shows the number of requests for information sent by the OMLP (in hard copies) between 2012 and 2016.

Table 6: **number of requests to the reporting entities submitted by the OMLP following the receipt of the STRs**

Year	Number of requests
2012	2092
2013	2606
2014	2854
2015	3047
2016	2844

146. The OMLP opens between 500 and 600 cases per year. On average between four to five requests for additional information have been sent per case.

147. LEAs request and obtain confidential financial information held by the private sector through a court order. Prior to obtaining such authorisation LEAs need to identify the financial institution or DNFBP which holds the relevant information. Given that the level of knowledge in financial matters

varies between different police units involved in investigating predicate crimes, it would be difficult and ineffective for some units to carry out an in-depth analysis of financial information. For this reason, in some instances Police units (other than the Economic Crime Division and the National Bureau of Investigation) indirectly obtain relevant financial information through the OMLP. Requests for financial information sent to the OMLP by the Police do not always trigger further intelligence; they mostly entail the provision of information. Nevertheless, this method communication/cooperation provides LEAs with quicker access to financial data. If the information provided is valuable for further investigative purposes, then judicial authorisation is needed to transform the intelligence into evidence. However, the discussions held on-site did not convince the assessment team that the OMLP and LEAs are proactive enough in seeking information on beneficial ownership. Moreover, it appears that financial information provided by the OMLP was mostly used for investigating the predicate criminality rather than ML.

148. The OMLP opens a case each time it receives a request from LEAs which concerns suspicion of ML/FT. Such requests are subject to an in-depth analysis which lasts on average 2 to 3 months. The analysis of STRs received from reporting entities is carried out in the same time-frame. In practice, in urgent cases the OMLP completes its analysis as soon as possible and within the timeframe agreed with other stakeholders. Therefore, 2-3 months represents only the average time needed to complete the analysis of complex cases involving numerous transactions and interconnected business relationships.

149. In addition to the information sent by the OMLP, the police actively use their own operative sources for financial intelligence, which mainly includes information gathered through the use of special investigative techniques (secret observation and tracking, fictive bribery, supervision of telecommunications, wire-tapping, etc.).

Between 2010 and 2015, the OMLP has disseminated 1177 cases concerning suspicion on ML and 12 cases concerning suspicion concerning FT. On average the OMLP has disseminated 85 cases per year to the Police and other competent authorities (mostly the Financial Administration) involving suspicion of the commission of other criminal offences or administrative violations. In total, 514 such cases were sent in the aforementioned time-frame. Overall, out of 1177 disclosures, prosecution was initiated in 105 cases involving 286 persons.

150. Once it has disseminated financial intelligence to the police, the OMLP cooperates intensively with LEAs. Investigators and OMLP analysts meet and discuss relevant issues as a matter of priority. All interlocutors met on-site considered this cooperation and the overall quality of information submitted by the OMLP as very good. The case in the box below demonstrates the OMLP's proactive role in seeking and gathering relevant information for ML investigation purposes.

Box 2: Actions by the OMLP to support ML investigations

To support the investigation of ML with drug trafficking by an organised criminal group as the underlying predicate offence, the OMLP undertook the following actions:

- it collected information on the business relationships of 16 customers (natural and legal persons) connected to the case;

- it collected financial information related to 28 bank accounts of natural and legal persons including money remitters (MoneyGram and Western Union);

- it detected cash deposits on the related bank accounts, their transfers to the bank account held by a minor from which the real estates was bought;

- it gathered information on real estate ownership of the persons concerned.

All together 114 answers from financial and non-financial institutions were received further to the above-mentioned initiatives.

Based on the analysis of the information received, the OMLP i*) sent requests for information to 9 foreign FIUs; ii) requested foreign FIUs to carry out the postponement of transactions (transactions on*

a Bitcoin account which were later approved by the court), and *iii) coordinated the exchange of information with other two foreign FIUs following the initiative of Slovenian LEAs to seize the assets.*

While seeking and gathering intelligence the OMLP permanently held consultations with LEAs. Eight disclosures/reports on ML suspicion were disseminated by the OMLP to the Police and the Prosecutor (indicating the suspicion of all three types of ML), further to its analysis. This case demonstrates the ability of the OMLP to seek, gather and analyse financial intelligence which is then used by LEAs in investigating and prosecuting the ML offence. The details of this case which concern the investigation and prosecution phase are described under IO.7 (see Box 5: ML case in relation to drug trafficking as a predicate offence, use of legal entities and virtual currencies).

151. Despite the facts noted above, there is a considerable discrepancy between the number of disclosures compared to the number of subsequent ML/FT investigations/prosecution/convictions. This mismatch does not stem from lack of capacity of the OMLP in developing financial intelligence or from poor cooperation with LEAs. The effective use of financial intelligence is directly linked to two factors which are not under the direct control of the OMLP and LEAs. The *first* factor is related to the analysis of STRs that concern transactions from a neighbouring country (referred as a specific typology under and elaborated in the Box 3 below). While banks have diligently reported these activities and the OMLP has analysed the related STRs, insufficient cooperation and information on the predicate criminality committed in the neighbouring country has prevented these cases from being further processed.

Box 3: Typology from country X

The funds are transferred from a neighbouring country to the accounts of natural persons or Slovenian shell companies which have accounts in Slovenian banks. Soon after the funds have been credited to the account, they are withdrawn in cash. While initially cash withdrawals were carried out in banks, further to changes in the regulations limiting cash withdrawals, other techniques have been used such as ATM withdrawals or the use of pre-paid cards. The origin of money is unknown and in most of cases such transactions are considered as suspicious. This typology concerns the entire banking sector. Whereas in most of cases banks are able to detect these transactions and file an STR, further information exchange aimed at identifying the predicate criminality, in general, has not yielded satisfactory results.

152. The *second* factor concerns issues related to: i) the evidentiary threshold for ML convictions further to the 2014 and 2015 Supreme Court decisions; and ii) amendments made to the Criminal Code in 2012 (Article 249 with regard to Article 99 of the CC)[47] . The impact of the verdicts of the Supreme Court on the use of financial intelligence has been considerable (the details are elaborated under IO.7). LEAs have perceived the 2015 judgement (Ips 59294/2010 of 18 June 2015) as introducing additional requirements with regard to the evidence needed to secure a conviction for ML. As a consequence, a significant number of OMLP disclosures have not been reported to the prosecutors as the criteria set by this jurisprudence were deemed to not have been fulfilled. These disclosures have therefore been set aside and stored to serve for information purposes only.

153. As concerns the amendments to the CC, they have not led to a decrease in the flow of intelligence related to possible tax evasion. They have, however, reduced the use of this intelligence for criminal investigations. More specifically, 516 disclosures were sent by the OMLP to the TARS between 2010 and 2016; this intelligence was mostly used for tax evidentiary purposes and not for investigating ML.

---

[47] The Criminal Code was amended in 2012 and the threshold for criminalisation of tax evasion was raised from 5,000 to 50,000 EUR. In 2015 new amendments were introduced and this threshold is now applicable to tax evasion carried out in a one year period.

154. LEAs have initiated a limited number of FT investigations. It appears that financial intelligence is more often used to pursue terrorism cases. SISA has reported that when there is a reasonable doubt that a terrorist attack may occur, the OMLP powers of gathering financial data have been used. Based on the information exchange with the OMLP, SISA gathers additional data by using the methods provided by the law (i.e. different types of technical surveillance and covert observation). Once preliminary checks have been completed, SISA exchanges information with the police and, if need be, with international partners. SISA representatives have advised that the OMLP has provided them with a variety of financial information that can be of relevance for a particular case (e.g. bank account details, transfers, etc.). However, the analysis of financial information is not carried out on a permanent basis; it is undertaken on case by case basis taking into account SISA's particular needs in the concrete case. No information related to proliferation has been disseminated by the OMLP so far.

155. The authorities have advised that the terrorism attempts investigated thus far have involved very limited financial resources and were most likely cases of self-funding. Therefore, the authorities have considered these circumstances as insufficient for initiating a FT investigation. Nonetheless, financial intelligence is duly analysed whenever terrorism financing suspicion arises. In view of the aforementioned and given the low number of suspicious activities concerning terrorism financing, the financial intelligence, so far, has not had a significant effect in preventing terrorism/FT.

STRs received and requested by competent authorities

156. The OMLPs' analyses are primarily based on STRs reported by banks (almost 90%). The STRs usually contain details of suspicious bank transaction(s) and other supporting banking information, such as the description of suspicious client behaviour and other relevant information. Usually the suspicious transactions are identified based on the indicators issued by the OMLP. These indicators were not, however, published on the OMLP website (at least on its English version) but were communicated to the reporting entities during the trainings held by OMPL.

157. The number of STRs received is relatively stable since 2012.

Table 7**: number of STRs received from the reporting entities (2010 – 2015)**

Reporting entity	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Financial and credit institutions	**172**	**251**	**491**	**532**	**411**	**453**
	96%	**96%**	**98%**	**98%**	**97%**	**97%**
Banks	164	238	461	504	372	422
Savings banks	5	7	16	12	25	19
Post Office	1	4	9	2	4	6
Securities firms	1	1	1	9	4	2
Insurance companies	-	-	-	-	1	3
Leasing companies	1	1	4	3	4	1
Other obliged entities	-	-	-	2	1	-
DNFBPs	**6**	**11**	**11**	**10**	**12**	**11**
Auditors and accountants	1	-	-	2	1	-
Casinos	-	-	-	-	2	2
Organizers of the games of chance	-	1	-	2	2	1

Dealers with precious stones	2	8	7	5	2	5
Real Estate Agencies	1	-	-	-	1	-
Notaries	1	-	2	1	4	-
Lawyers	1	2	2	-	-	3
TOTAL	**178**	**262**	**502**	**542**	**423**	**464**

158. The OMLP has advised that STRs filed by the banks are of a good quality. The STR forms – regardless if they are electronic[48] or hard copies - require the reporting entities to provide considerable information on the suspicious transaction, CDD records, data on the person on whose behalf the transaction has been performed or initiated and data on the reasons for suspicion. Usually the STRs contain all the data which is necessary to identify the client and the persons on whose behalf the client is acting. The STR explains why the particular transaction is considered as unusual/suspicious in connection with the client, particular business or other transactions performed by the client. The STRs are submitted together with the supporting documents (identification of client, banking information, contracts, invoices, etc.).

159. Nevertheless, the OMLP estimates that around 20% of STRs they receive have certain quality shortcomings. In addition, BoS has indicated a number of infringements with regard to the quality of information/STRs submitted by banks, which it has discovered while performing its role as banking supervisor. The OMLP does not provide feedback on the quality of individual STRs. On the other hand, the feedback to banks on this matter is provided during the annual meetings where analysis of STRs, received in a year's time, is presented and discussed with compliance officers. The STRs received from other sectors including the non-banking financial institutions and the DNFBPs does not have a significant impact on the quality of the financial intelligence, given the low percentage of such STRs compared to the overall statistics of STRs submitted.

160. In addition to STRs, the OMLP receives information from the customs database, which contains cross border currency and bearer negotiable instruments declarations collected from travellers and gold transactions. However, in the past few years Customs has not sent the OMLP any reports on suspicious cross-border transportation of currency or bearer negotiable instruments. In the authorities' view, this is due to the fact that Slovenia borders only with EU countries. Nonetheless, three airports and one harbour receive international travellers and goods. The OMLP also receives aggregated data from FIs (CTR; wire transfers exceeding 30.000 EUR when the receiving subject have his/her/its residence or seat in a country with higher ML/FT risk, regardless where the actual destination of transfer is; wire transfers exceeding 30.000 EUR when assets are transferred to a financial institution in a country with a higher ML/FT risk).

Operational needs supported by FIU analysis and dissemination

(a) Operational analysis

161. The OMLP opens a case upon receipt of an STR (between 2010 and 2015 the OMLP has opened 2720 cases on the base of the 2747 STRs received). A case can also be opened when reports/inquiries are received from governmental institutions, foreign FIUs and data mining of CTRs. The operational analysis is carried out by experienced and well-trained analytical personnel of the OMLP. Eight staff members perform operational analyses.

[48] The electronic form is yet to be introduced. However, during the on-site visit, the electronic form was in a 'testing' phase, nevertheless the assessment team had a chance to see it and examine its content. It presents step forward not only in terms of technology used but also in terms of data that need to be submitted. Up to the on-site timeframe, the hard copy form was still in use.

162. However, there is no analytical methodology available to the OMLP staff providing guidance on how to conduct the process. The assessment on how information should be collected and analysed is left to the discretion of the staff member in charge.

163. The head of department and the director of the OMLP are involved in all of the phases of the analytical process. More precisely, each STR is first checked by the OMLP director and then by the head of the analytical department. Only then it is assigned to an analyst. The head of department, as per his discretion, assigns the case to an analyst.

164. As a matter of practice, cases/STRs are assigned to analysts based on their specific expertise – e.g. FT cases are assigned to an analysis specialised in FT, while some specific STRs (e.g. 'neighbouring country typology' STRs) are assigned to an analyst specialised in that particular matter. The level of specific AML/CFT expertise among staff members differs significantly (Table 8).

Table 8: **Expertise of the OMLP analysts**

Employee	Years of experience in OMLP	Background
1	17	Police
2	17	Police
3	10	Police
4	5	Tax Authority
5	2.5	Ministry of Finance
6	2	Police
7	1.5	Ministry of Finance
8	1	Police

165. The analytical process includes checking all the electronically available databases. Based on the personal discretion of the analyst in charge, further information may be requested from the relevant reporting entity/ies or governmental authority/ies (in a hard copy form) even in this phase. Requests to foreign FIUs are sent when cases contain a significant international element. Once the initial information-collection phase has been concluded, the case is discussed between the analyst in charge and the head of the analytical department, who gives further instructions. These instructions are mandatory and may include the collection of additional data, disclosing the case to LEAs or closing the case if the initial suspicion has not being confirmed. The final decision is made by the Director of the OMLP.

166. The overreliance on the analytical skills and expertise of the employees does not have a negative impact on the quality of the analysis as all phases of the analytical process are directly supervised. Nonetheless, the evaluation team deems that the OMLP would benefit from a written analytical methodology as it would ensure the consistency of the analytical process and would prevent the potential loss of institutional memory in case of staff changes.

167. The capacities of the AML/CFT analytical departments, in terms of human resources available, may be an issue of concern given the overall workload. The statistics on STRs (including the requests for information coming from foreign counterparts) submitted between 2012 and 2016 and the average time period needed for the subsequent analysis support this conclusion.

168. The ability of the OMLP to postpone transactions has also been used by the Police and prosecutors. Although this is an OMPL power, in practice it has been applied upon the request of LEAs with the aim to secure the proceeds of crime and to avoid their 'migration' at the early stage of investigation. Overall, in the period 2011-2016, the OMLP has issued 79 postponement orders to suspend transactions or block an account. LEAs do not consider the temporary postponement of

transactions to be a sufficient tool for asset recovery initiatives (e.g. securing the confiscation of crime proceeds). This is due to the short period of validity of the measure as it is unlikely to provide LEAs with sufficient time to gather the evidence needed to obtain a court order for securing the assets; and, on the other, the limited scope of the measure, which is only available for ML/FT cases and not for other types of proceeds-generating crimes.

(b) Strategic analysis

169. Strategic analysis is carried out by two OMLP analysts. OMLP reported that in 2016 three analyses have been produced, mostly related to ML/FT trends and typologies such as the use of off-shore companies and offshore movement of funds.

170. OMLP has issued the document which aims to provide the OMLP staff with a better understanding of the requirements and evidence threshold set by the jurisprudence and the Criminal Code. However, it does not set mandatory obligations for the analytical work of the OMLP and it is not considered as strategic analysis within the meaning of FATF standards. The guideline recommends specifying the elements of the ML offence when disclosures are sent to police. The guidance has therefore also been presented to the Police in the course of the trainings provided by the OMLP. The Police has been advised to use the same principle when preparing and submitting criminal complaints to the Prosecutor's Office. Overall, certain common features should accompany both police and OMLP analysts in this endeavour. These include the need to establish that: (1) the suspect knows that the assets which are the subject of a transaction/arrangement derive from criminal activity(ies); (2) the suspect has initiated the laundering process knowing that the proceeds have been illegally obtained ; (3) the assets have been disposed by the suspect; (4) the aim of the transactions or arrangements is to hide the true origin of the assets (*e.g. ownership, transfers, straw man, beneficial owners, cash withdrawals, cross border element, etc.*); (5) the OMLP and Police should describe the phase in which the money laundering process has been carried out so that the judicial authorities can distinguish the concealment and the laundering phases. Similar guidance was prepared by the OMLP for some other criminal offences including the financing of terrorism (together with other terrorist related criminal offences).

171. In addition, the OMLP takes active part and prepares/participate in the preparation of the strategic analysis/documents of the governmental working groups and committees. As noted under IO1, the OMLP is considered by the authorities as a key AML/CFT coordinator and policy making/proposing body in Slovenia.

(c) Disclosures

172. The OMLP provides information to LEAs on a spontaneous basis (at its own discretion), both in instances linked to on-going investigation and in cases which identify potential targets.

173. One case can contain a number of STRs linked together by subjects or transactions. The reports are sent in written form and include the relevant documents (as a matter of practice these documents are sent in hard copies; now it is also done in electronic or CD format). The information exchange (in hard copies) between the OMLP and the Police concerning the disclosures on STRs is classified under the one of four possible confidentiality levels – "INTERNO" (Restricted), "ZAUPNO" (Confidential), "TAJNO" (Secret) and "STROGO TAJNO" (TOP SECRET).

(d) Pre-investigation phase

174. The OMLP disclosures are checked by the Police in the pre-investigative phase during which the Police collects information which can justify the initial suspicion and lead to the opening of an investigation in accordance with the CPC. The Police usually consult the prosecutor during the pre-investigative phase and coordinate their actions in line with the prosecutor's instructions. The Prosecutor decides if and to what extend he/she should be involved in providing legal advice if the evidentiary threshold for the initiation of the formal investigation has been reached. Firstly, the Police check the disclosures and match them with existing information in the available databases. Based on this analysis the police decide whether or not to submit a criminal complaint on ML.

Nonetheless, whenever Police decide not to submit a criminal complaint, the prosecutor has to be informed.

175. Between 2010 and 2015 (Table 9 below), 290 ML criminal complaints/reports were sent by the Police to the Prosecutor's Office is. 42% of them (or 123 complaints/reports) were sent based on information/disclosures received from the OMLP, while OMLP disclosures/information were the basis for 118 criminal complaints submitted by the police to the Prosecutor's Office for criminal offences other than ML. In 170 cases the Police informed the Prosecutor's Office that there were no reasons to suspect that criminal activity had occurred. Last but not least, in 160 cases LEAs used the OMLP intelligence as operational information in their own inquires/cases.

Table 9: **ML criminal complaints on ML submitted to the Prosecutors in period 2010-2015**

Type of activity	**Criminal complaints on ML sent by Police to Prosecutor**	**Criminal complaints sent by Police to Prosecutor based on OMLP disclosures** (*part of the aforementioned 290*)	**Other criminal complaints (for crimes other than ML) sent by Police to Prosecutor based on OMLP disclosures**	**Cases, where Police informed Prosecutor that there were no reasons to suspect any criminal activity**	**Number of cases where OMLP disclosures were stored by LEAs for information purposes**
Number	290	123	118	170	160
Year	**Number of suspected**			**Approximated amount of laundered money**	
	Natural persons	**Legal entities**			
2010	107	7		97.157.172 €	
2011	77	21		24.406.713 €	
2012	85	22		70.585.263 €	
2013	125	23		64.927.102 €	
2014	103	17		28.823.599€	
2015	78	15		22.088.176 €	

Cooperation and Exchange of Information/Financial Intelligence

176. The OMLP, Police and other relevant governmental authorities cooperate and exchange information and financial intelligence on a regular basis. LEAs and judicial authorities regularly provide the OMLP with statistics concerning ML/FT cases they have dealt with. The Police, on an annual basis, collect and send to the OMLP data on on-going ML investigations. This data is then used by the OMLP for both strategic and operational analysis. The OMLP receives feedback from the Police also on a case-by-case basis when an investigation has been conducted. This feedback however does not include additional information on how the financial intelligence has been supplemented by LEAs through the use of its investigative means. Furthermore, the OMLP does not receive feedback from LEAs on whether the analyses provided were useful and how they can be improved.

177. Despite the difficulties encountered, both the OMLP and Police consider their cooperation as fruitful and effective. During the on-site visit, the assessment team was provided with a number of

examples in which the specific knowledge/expertise of the OMLP staff was used by other agencies and special investigative teams.

178. The OMLP and the Police are currently involved in 8 ML/predicate offence investigations. These investigations are carried out by special investigative teams and are under the direct supervision of the prosecutor. Each of these cases includes transnational element(s). The Authorities have further advised that between 2010 and the end of 2016, the OMLP has participated in 34 special investigation teams. At least 18 OMLP disclosures on ML suspicion were the basis for further investigations in the afore-mentioned 34 joint investigations.

179. The OMLP and the Police cooperate in the following cases: when during the analytical process the OMLP analysts establish a link with an on-going investigation, the Police is informed and additional steps are proposed; The Police seeks cooperation with the OMLP during the pre-investigative and investigative phases when financial analysis is required or when it needs to collect data through the OMLP channels for international cooperation. LEAs consider the OMLP channel as the most effective to obtain financial information from abroad. However, the OMLP has informed the evaluation team that in some instances the above-mentioned financial information cannot be obtained given the insufficient assistance provided by some European (EU and non-EU) FIUs. In complex cases which include foreign elements, this information can be of key importance to both LEAs and the judiciary.

180. All the information related to STRs, financial information and any other information of relevance is stored (electronically or in hard copy) in the OMLP database. The information system is independent and has no connection outside; access to it is protected by password. The OMLP premises can only be accessed by OMLP staff and through a personal electronic card.

181. All OMLPs databases are stored in ORACLE while data mining is possible with standard applications like MSquery, SQL Plus. In 2016 the OMLP started to introduce a new IT system based on PostgreSQL technology. The system can automatically request data and store it together with other information related to the same case, create some basic case files, inter-connect them, and receive data from obliged entities/institutions. All operational analysis in performed in Excel Pivot Tables.

182. The authorities have reported that there has been no breach of the confidentiality of financial intelligence. All LEAs treat the information received from the OMLP in line with its level of secrecy and the respective requirements of the Law on Classified Information.

183. With regard to FT related issues, the OMLP cooperates on a regular basis not only with LEAs but also with SISA. The authorities have reported that the level of communication is valuable for both sides. On the one hand, the OMLP receives operational intelligence which can be incorporated in its analyses; on the other hand, SISA can use the information on financial flows received from the OMLP for its own purposes, including to identify specific connections between persons. SISA analyses can serve as intelligence and can be used by LEAs to initiate FT related investigations.

Overall Conclusions on Immediate Outcome 6

184. The OMLP and the Police have access to a wide range of financial information and other information gathered by governmental bodies. The information and subsequent analysis prepared by the OMLP mostly serves LEAs in the pre-investigatory phase of ML/FT inquiries.

185. The DNFBP sector has a very low level of suspicious transactions reporting; this may be linked to the low level of awareness concerning its obligations in preventing ML/FT. The authorities also do not seem to be proactive in seeking/requesting such information from DNFBPs.

186. The effective use of financial intelligence by the OMLP and the Police is affected by the standard of proof set by the jurisprudence which LEAs perceive as high, and by the current legal framework. While significant efforts are invested both by the OMLP and the police to analyse financial

intelligence, the majority of disclosures received from the OMLP is stored in LEAs databases and serves for intelligence purposes only.

187. Further specialisation of the Police units dealing with predicate criminality is needed to carry out parallel financial investigations more effectively. So far LEAs have mainly focused on gathering evidence on the predicate criminality, and only then (i.e. once sufficient evidence on predicate offence is gathered) in tracing the criminal assets and property laundered.

188. Financial intelligence is used to develop evidence and trace criminal proceeds to some extent. Most information provided by the reporting entities and foreign FIUs (STRs and foreign financial intelligence) is used by the OMLP for operational analysis, and, to some extent, for strategic analysis. Although LEAs are satisfied with the quality of information received and the cooperation with the OMLP, statistics show that the number of disclosures triggering criminal investigations is not particularly high. This however, cannot be considered to be the direct result of lack of capacity of LEAs but is more related to the legal and other contextual factors in Slovenia.

189. Although the OMLP has at its disposal qualified and skilful analysts, the overall amount of work compared to the number of staff assigned suggests that the analytical department is insufficiently staffed.

190. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 6**.

Immediate Outcome 7 (ML investigation and prosecution)

191. ML investigations are conducted by the Financial Crime and Money Laundering Section (FCMLS) of the Criminal Police Directorate (which includes eight Regional Police Directorates and their Economic Crime Sections – Financial Crime Groups), the regional police directorates, police units at the local level, and the National Bureau of Investigation (NBI). The FCMLS is a specialised police unit responsible for combating financial crime and ML at the state level. In addition, it oversees, coordinates, analyses and supervises the work of the police directorates in charge of combating financial crime. The NBI is a specialised criminal investigation unit at the state level established within the General Police Directorate which detects and investigates more complex cases of economic and financial crime, corruption and other forms of organised crime which require international or inter-institutional cooperation.

192. Investigations are carried out by the police under the prosecutor's supervision and guidance. As a general rule, the police informs the prosecutor of the cases they have opened and the Prosecutor provides instructions on the investigative actions that need to be undertaken.

193. Under the CPC, the head of the competent Prosecutor's Office may establish a special investigation team (SIT) when investigating complex crimes, especially when the expertise of other state authorities in the area of taxes, corruption, customs, financial operations, securities, ML, organised crime, public procurement abuses and trafficking in narcotic drugs is required. The competent State prosecutor manages and directs the investigative action of the SIT, whose members are appointed by the heads of the competent institutions. The State prosecutor includes, for example, tax authorities in the special investigation team if: i) he/she deems that a parallel financial investigation is needed in the particular case (when criminal offence results in a material benefit); ii) when temporary measures for securing assets have been taken in order to secure confiscation at a later stage; iii) he/she deems that the collection of financial data is necessary in order to decide whether to issue an indictment. In the reference period 12 SITs have been formed and six are still operational. All agencies met on-site consider this platform of cooperation as a useful tool for investigating/combating serious crime.

Box 4: Example of an SIT

In 2013 the head of the State Prosecutor's Office in Maribor set up a SIT including experts from the Criminal Police, the Tax Authority, the Ministry of Finance, the OMLP, the Ministry of Economic Development and Technology, the Market Inspectorate and the state prosecutor in

relation to a case of alleged usury, fraud and money laundering committed by several natural and legal persons. The SIT's mandate was to collect evidence and the necessary information to decide whether to initiate criminal proceedings against the suspects and to file a criminal report. As a result of the SIT's work, the State Prosecutor's Office in Maribor filed an indictment in December 2016 against six persons (two natural and four legal persons) for committing the continuous crimes of usury, fraud, embezzlement and unauthorised use of another's property. The criminal proceedings are still underway.

ML identification and investigation

194. The agents of the FCMLS and of the NBI are trained in conducting financial investigations and in pursuing ML in the context of such investigations (financial investigations are further elaborated under IO.8 below). The FCMLS has issued a number of instructions and guidance in relation to the investigation of ML, including on how to file ML criminal reports, cooperate with the OMLP, investigate ML offences which involve suspicious transactions carried out by nationals of certain countries etc. Nonetheless, there are no policy documents compelling the NBI to prioritize ML cases and the evaluation team was informed that the police unit which is competent to combat trafficking and production of narcotic drugs does not systematically pursue ML in the context of parallel financial investigations, focusing rather on apprehending the suspect and seizing the drugs. A comparison between the number of convictions for predicate offences and the number of ML investigations indicates that in practice LEAs do not often pursue ML in connection with predicate offences. For instance, in 2010 a total of 1802 natural/legal persons were convicted for predicate crimes, whereas 44 ML investigations against natural/legal persons were opened by LEAs independently (not on the basis of an STR).

195. The identification and investigation of potential cases of ML are triggered either by reports disseminated by the OMLP or by the investigation of a predicate proceeds-generating offence, which in its turn is activated by a complaint, report, or on the basis of law enforcement intelligence.

196. As concerns OMLP disclosures, as indicated under IO.6, although LEAs are satisfied with the quality of information received from the OMLP and the overall cooperation with this institution, a low number of OMLP disclosures triggered further investigation/prosecution. This is a result of the fact that, on the one hand, many STRs are related to the Typology of Jurisdiction XX (see IO2 and IO7 concerning the problems encountered in this respect) and, on the other hand, that the standards of proof set by the jurisprudence are perceived as being considerably high (see IO6 in this respect). OMLP disclosures often detect ML cases without identifying the underlying predicate criminal offence, thus these disclosures do not trigger investigations unless additional information/evidence has been obtained to further substantiate it.

Table 10: **ML and FT cases statistics (concerns the cases initiated upon submission of disclosures by OMLP)**

	OMLP Cases in the reference year				Related judicial proceedings in reference year – Number of cases				Related judicial proceedings in reference year – number of persons			
					Prosecution*(based on OMLP disseminated cases)		Convictions (final)		Prosecution* (based on OMLP disseminated cases)		Convictions (final)	
	STRs Under analy	STRs Archived in refere		Reports disseminated for investigation	ML	FT	ML	FT	ML	FT	ML	FT

	sis at year end	nce year										
2010	207	**109**		77	**12**	**0**	**2**	**0**	**37**	**0**	**3**	**0**
2011	255	**98**		132	**23**	**0**	**2**	**0**	**72**	**0**	**2**	**0**
2012	378	**130**		196	**20**	**0**	**7**	**0**	**72**	**0**	**16**	**0**
2013	436	**155**		219	**21**	**0**	**1**	**0**	**48**	**0**	**1**	**0**
2014	522	**208**		268	**20**	**0**	**4**	**0**	**37**	**0**	**9**	**0**
2015**	572	**206**		285	**9**	**0**	**0**	**0**	**20**	**0**	**0**	**0**

*Instead of prosecution we use number of criminal complaints filed by Police to Prosecutor

** Data for 2015 are not final yet

197. Police-generated ML cases often have abuse of power in business operations as the underlying predicate offence. Investigation of such cases is typically initiated when the police receives information that a company director has transferred money abroad without a legitimate reason. As indicated above, the NBI is responsible for investigating complex crimes which generate large amounts of criminal proceeds. The evaluation team was informed that the NBI carries out parallel financial investigations when investigating a predicate crime and, in this context, looks into whether ML elements are present. The NBI may request that the OMLP provide additional information or analysis in order to establish i) whether the suspect holds illegal proceeds; ii) if attempts to conceal the origins of funds were undertaken; and iii) and if any attempt to move the proceeds has been made so that it can carry out additional actions for confiscation purposes. In the course of the investigation, the NBI can closely cooperate with the Financial Administration to obtain the necessary information. This cooperation has proved to be very useful, especially in organised crime cases. As indicated in the paragraphs above, however, it is not clear the extent to which parallel financial investigations are carried out as a matter of practice.

198. The statistics provided by the authorities on the crime reports submitted to the State prosecutor by the Police (please see Table 9 in IO6) indicate that in 2015 there was a decrease in the criminal complaints on ML submitted by the police to the prosecutor. This trend is perhaps also the result of the Supreme Court decision from 2015 which is purported to have raised the evidentiary standards in relation to ML (please see the analysis under Types of ML cases pursued). LEAs face a number of additional obstacles in pursuing ML investigations as outlined under Core Issue 7.3.

199. A significant number of legal persons have been investigated for ML, however only 3 cases were taken further and were subject to court proceedings. In the past legal requirements to set up companies were not stringent, thus companies would be set-up for criminal purposes, operate for a limited period and shortly afterwards be deprived of their assets and left as dummy companies. The authorities thus considered that there would be no added value in pursuing these companies for ML given the absence of assets which could be confiscated. In addition, it appears that authorities tend to focus more on natural persons as the perpetrator of ML criminal offences.

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

200. According to the Slovenian NRA, the domestic economic crimes which are deemed to pose the highest ML threat are abuse of position or trust in the performance of economic activities, tax evasion, business fraud and abuse of official position or official duties. Outside of the realm of economic crime, offences related to illicit drugs are deemed to pose the highest ML threat. As indicated under IO.1, certain ML risks have not been sufficiently analysed, including tax evasion crimes involving foreign elements.

201. ML investigations and prosecutions reflect to some extent the risks that the country faces. ML investigations are mostly linked to the investigation of criminal offences in the field of economic crime. As is highlighted in the statistics below, domestic tax evasion is one of the most frequent underlying predicate offences to ML, followed by abuse of position or trust in business activity, fraud/business fraud. On the other hand, Slovenia's risk profile would warrant a higher number of ML investigations related to foreign tax predicate offences, corruption offences, drug offences and organised criminality. As noted in IO2 and later in the analysis, obstacles in receiving information from a neighbouring jurisdiction has hindered the investigation and prosecution of ML with foreign tax evasion as the alleged underlying predicate offence (Jurisdiction X Typology). As concerns the investigation of ML with drug offences as the underlying predicate crime, in the period under review only four investigations were opened. Indeed, the evaluation team was informed that the police unit which investigates the trafficking and production of narcotic drugs does not systematically pursue ML in the context of parallel financial investigations.

Table 11**: Predicate offences underlying money laundering investigations:**

Article (Criminal Code-CC)	**Predicate criminal offence**	**CO 2010**	**CO 2011**	**CO 2012**	**CO 2013**	**CO 2014**	**CO 2015**	**Total**
254 CC / 249 CC-1	Tax evasion (domestic)	25	25	14	6	5	8	83
244 CC / 240 CC-1	Abuse of Position or Trust in Business Activity	10	8	8	10	13	12	61
212 CC / 205 CC-1	Grand Larceny	8	1	11	14	4	1	39
234a CC/ 228 CC-1	Business Fraud	2	/	3	4	3	5	17
212 CC-1	Organising Money Chains and Illegal Gambling	/	/	2	/	/	/	2
217 CC/ 211 CC-1	Fraud	/	/	1	8	8	5	22
213 CC/ 206 CC-1	Robbery	/	/	1	/	/	/	1
233 CC	Causing of bankruptcy by business mismanagement	/	/	1	/	/	/	1
209 CC-1	Embezzlement	1	1	1	2	/	/	5
306 CC-1	Manufacture and Acquisition of Weapons and Instruments Intended for the Commission of	1	1	3	/	/	/	5

	Criminal Offence							
235 CC	Fraud in Obtaining Loans or Benefits	1	/	/	/	/	/	1
247 CC	Unauthorised Acceptance of Gifts	1	/	/	/	/	/	1
196 CC/186 CC-1	Unlawful Manufacture and Trade with Narcotic Drugs	/	/	1	2	1	/	4
183 CC-1	Manufacture and Trade in Harmful Remedies	V	/	1	/	/	/	1
261 CC-1	Acceptance of Bribes	/	/	/	1	/	/	1
227 CC-1	Defrauding Creditors	/	/		1	/	1	2
261 CC	Abuse of Office or Official duties	/	/	/	2	1	1	4
229 CC-1	Fraud to the Detriment of European Communities	/	/	/	1	2	1	4
247 CC-1	Use of a Counterfeit Bank, Credit, or Other Card	/	/	/	1	2	2	5
244 CC-1	Fabrication and Use of Counterfeit Stamps of Value or Securities	/	/	/	/	3	/	3
243 CC-1	Counterfeiting money	/	/	/	/	3	/	3
254 CC-1	Illegal Provision of Legal Aid	/	/	/	/	/	1	1
208 CC-1	Misappropriation	/	/		/	/	1	1
241 CC-1	Unauthorised Acceptance of Gifts	/	/	/	/	/	1	1
CC in foreign countries	Tax evasion, Abuse of Position or Trust in Business Activity Smuggling	/	/	8	4	3	2	17
CC in foreign countries	Foreign predicate offences related to Drugs	/	/	1	/	/	/	1
CC in foreign countries	Foreign predicate offences related to tax evasions	/	/	1	4	/	/	5
CC in foreign countries	Foreign predicate offences related to fraud	/	/		3	/	/	3
CC in foreign countries	Foreign predicate offences related to smuggling	/	/	/	1	/	/	1
CC in foreign countries	Foreign predicate offences related to unauthorised Acceptance of Gifts	/	/	/	1	/	/	1

202. The FCMLS has indicated that, as far as the cases they have investigated, the most common predicate offences to ML include different types of economic and other profit generating crimes, such as tax evasion, business fraud, cybercrime and drug trafficking and that some of these crimes are committed by organised criminal groups. The prevailing predicate offence in ML investigations led by the NBI, on the other hand, has been the abuse of trust in economic activities. The NBI has also investigated some corruption cases in the health sector involving bribes given to doctors by pharmaceutical companies in return for being selected in procurement procedures. Contrary to the information provided by the FCMLS and the OMLP, Supreme Court representatives indicated that drug trafficking and abuse of power in the economic sector were the most recurrent predicate offences to ML, more so than tax evasion.

203. Indeed, the United Nations Office on Drugs and Crime (UNODC) has reported that Europe is increasingly a destination for heroin along the southern route through Africa, impacting also East and Central Europe. Slovenia has carried out its first seizure of heroin related to this route in 2012[49]. The authorities also mentioned the recent seizure of 865 kg of narcotic drugs. This case and the action taken by police were reported in the media. The assessment team was informed by the authorities that an in-depth financial investigation was initiated. Whereas the investigation is still undergoing, no indication has been given as to whether an investigation into the presence of ML elements has been undertaken.

Box 5: ML case in relation to drug trafficking as a predicate offence, use of legal entities and virtual currencies

A number of criminal complaints against several persons were submitted to the public prosecutor for suspicion of Unlawful Manufacture and Trade of Narcotic Drugs, Illicit Substances in Sport and Precursors to Manufacture Narcotic Drugs (Article 186 of the CC). The crime was committed by an organised criminal group (OCG); its members dealt and sold the illicit drugs on the Internet to customers from over 39 countries. Three methods of payment were available to the buyers: the payment to a foreign bank account, Bit coin transfers and through Western Union. Criminal complaints against some of the suspects were also submitted for suspicion of ML (Article 245 of the CC) given that the proceeds of the underlying crime had been transferred to the account of a Slovenian shell company and then to the accounts of other off-shore companies which the OCG had founded for criminal purposes. Assets which had been acquired with Bit coins and through Western Union were exchanged for cash. Some of these funds were deposited in bank accounts, including in the bank account of a family member of one of the suspects (a minor). Funds from this account were later used by the suspects to pay a security deposit for purchasing at least three apartments to be put up for rent, and to buy real estate abroad (in Austria). Some of the proceeds were transferred from one company to another on the basis of fictitious service contracts and invoices and part of these sums was later purported to be used as the salary of one of the suspect for legitimate business carried out for a financial institution. In addition, one of the suspects kept substantial sums of cash in his apartment at the time of search. Real estate was also purchased for OCG's family members, part of which was later sold to bona fide purchasers. The proceeding is still on-going. In the context of this case, the OMLP performed a number of actions including the: collection of financial information related to 28 bank accounts of 16 natural and legal persons, including money remitters; collection of information from nine FIUs; coordination and exchange of information with other two FIUs in relation to the seizing of assets. As a result, the OMLP sent the police and the Public Prosecutor 8 reports regarding suspicion on the commission of three types of ML (cash deposits on bank account held by a minor used to buy real estates; investment of funds in a company; and Use of BITCOINS). During the police investigation, undercover measures were used.

[49] UNODC, *World Drug Report* 2015, https://www.unodc.org/documents/wdr2015/World_Drug_Report_2015.pdf and UNODC report *Afghan opiate trafficking via southern route*, https://www.unodc.org/documents/data-and-analysis/Studies/Afghan_opiate_trafficking_southern_route_web.pdf

Types of ML cases pursued

204. The statistics shown in the Table below demonstrate that in the period under review the authorities have made progress in securing ML convictions. According to this table the majority of ML convictions (54,1%) were for third-party laundering which demonstrates that the authorities, to some extent, go beyond the perpetrator of the predicate offence, conduct financial investigations and detect, prosecute and convict third-party money launderers. However, a significant number of such third-party ML cases were related to computer fraud and similar offences in which only the "mules" could be apprehended as the perpetrators of the predicate offence remained unknown. There were only three judgements against legal persons.

Table 12: **Analysis of convictions for AML/CFT cases**

Year	Cases	Total number of ML convictions	Number of convictions for self laundering	Number of convictions for third party laundering+	Number of convictions for laundering proceeds of crime committed abroad	Number of convictions for fiscal predicate offences	Number of convictions for non-fiscal predicate offences
2010	**0**	**0**	**0**	**0**	**0**	**0**	**0**
2011	**2**	**3**	**1**	**2**	**0**	**0**	**3**
2012	**4**	**6**	**2**	**4**	**0**	**0**	**6**
2013	**17**	**19**	**12**	**7**	**1**	**3**	**16**
2014	**16**	**21**	**13**	**8**	**1**	**1**	**20**
2015	**14**	**25**	**6**	**19**	**0**	**0**	**25**
31.3. 2016	**0**	**0**	**0**	**0**	**0**	**0**	**0**
Total	**53**	**74**	**34**	**40**	**2**	**4**	**70**

205. The evaluation team was informed of three convictions for stand-alone ML in 2013 and 2014, two in which the predicate crime had not been fully identified but could be deduced by the facts of the case and one in which the predicate offence had not been identified and which referred to funds originating from crimes committed abroad. Furthermore, an important decision of the Slovenian Supreme Court was issued in 2014 (case No. I Ips 75110/2010 of 10 July 2014) clarifying the evidentiary requirements needed to prove ML, and facilitating proof of stand-alone ML. In the case at issue the defence had argued that the State prosecution had not proved that the property originated from crime, given that the first instance judgment had not identified the exact predicate offence or established that criminal proceedings had been instituted and a conviction had been issued. The Supreme Court found that in order to prosecute and convict for ML a prior conviction is not needed and that the determination of objective factual circumstances regarding the execution of the predicate offence is sufficient. Notwithstanding the above information, LEAs have informed the assessment team that in practice it is very difficult to pursue autonomous ML cases as charges are not pressed unless there is clear evidence that the predicate offence has been committed. This can perhaps also be attributed to the Supreme Court decision issued in 2015 (Ips 59294/2010 of 18 June 2015) which has been perceived as reversing the more flexible approach taken in the past on proving the predicate crime to ML.

206. The authorities have not provided a break-down of the convictions handed down according to the underlying predicate offences. Most of the convictions which have been handed down are for non-fiscal predicate offences (94,6%) which to some extent is at odds with the findings of the NRA and the fact that ML investigations with tax offences as the underlying predicate offence represent the largest share of opened ML investigations. The evaluation team also received contradictory information from different authorities concerning the number of ML convictions in relation to drug trafficking as the NRA would warrant a higher number of such cases. Nonetheless, in the period under review, a number of convictions have been secured for ML related to the abuse of position or trust in business activity, tax evasion, fraud and abuse of official position, in line with the risks that the country faces.

Box 6: Self-laundering and third-party ML case

The defendant, a lawyer who had been appointed as the insolvency administrator of a company, transferred 2,393,258 EUR to two foreign and one Slovenian company without any business logic. These companies were managed by family members of the lawyer. The insolvency administrator was found guilty of money laundering and was sentenced to three years of prison and, concurrently, was convicted to a term of imprisonment of six years for the underlying predicate offence and to a fine of 20,115 EUR. The insolvency administrator was also sanctioned with the prohibition of performing the duties of a liquidator for a period of five years and, by the bar association, with the removal of his licence to practice law. Property of 2,252,201 EUR was also confiscated (3x OA Mercedes Benz and real estate in Croatia). Three other persons who had acted as the managers of the three companies which had received the proceeds were also convicted for money laundering. One of them was sentenced to one year and a half of prison and a fine of 10,057 EUR; the other two were sentenced to one year of imprisonment each and a fine of 20,000 EUR and 30,000 EUR respectively. An appeal was filed against the first instance court decision. The court of appeal confirmed the first instance court decision and found additionally the main defendant guilty of business fraud and abuse of office and official duties. The lawyer was convicted by the Court of Appeals and was handed down a combined sentence of six years of imprisonment and a combined fine in value of 45,258,74 EUR. Confiscation of 2,132,883.77 EUR was also decided. The Court of Appeal also acquitted two defendants who had been convicted for money laundering and confirmed the ML conviction for the third defendant, and reduced his sentence to one year.

Box 7: Stand-alone ML case involving fraud as the underlying predicate offence

In 2012 an investigation was opened for suspicion of ML (under paragraph 1 of Article 245 of CC). The suspect received money knowing that it was proceeds of crime, used it and concealed its origin. The suspect had received two money orders to the Austrian bank accounts of his/her company (registered in Serbia). The first order was made by a German company and the second one by a Montenegrin company. These money orders originated from fraud under paragraph 1 of Article 211 of CC and to the detriment of German and Montenegrin companies. The fraud had been committed by unknown perpetrators using the Internet. The perpetrators had published an ad in the name of Company X advertising the sale of cargo vehicles. The representatives of the German and Montenegrin injured companies responded to the advertisement and were promised 2 MAN cargo vehicles against an advance payment. The cargo vehicles were not delivered and the companies were not reimbursed. Once the money had reached the Austrian bank account of Company X, the suspect made cash withdrawals. Immediately after these cash withdrawals the suspect transferred the money to Slovenia and transferred it to a third person. When executing the cash withdrawal the suspect knew that the money was acquired unlawfully, therefore, a criminal complaint for money laundering under paragraph 1 of Article 245 of CC was filed against him.

Following the trial, the court convicted five persons for committing fraud and ML: three

defendants were convicted for both fraud and ML, one only for ML and one only for fraud. All of the defendants were sentenced either to imprisonment or to suspended sentences together with a fine. Confiscation of 5,800.00 EUR has also been enforced.

207. The evaluation team was informed of a number of obstacles faced by prosecutors and judges in prosecuting and judging ML cases (see also the analysis of IO2 and IO6). Practitioners have indicated that a judgment of the Supreme Court issued in 2015 (Ips 59294/2010 of 18 June 2015) seems to have reversed the stance taken earlier on proving the predicate crime to ML (whereby the determination of objective factual circumstances regarding the execution of the predicate offence is sufficient) and has raised the level of proof needed for the underlying predicate offence in order to pursue ML.

208. Further discussions held by the assessment team with the judiciary authorities about the 2015 Supreme Court judgment, however, did not lead the team to the conclusion that indeed the judgment raises the level of proof required, although the practitioners' impression that it does, is a cause for concern. In the specific case, director A had transferred money from company X to the owner B of company Y. A was convicted for abuse of power in economic activity. B was charged both with incitement of abuse of power and money laundering. The judgement found that the incitement of the predicate offence by person B had not been proved and that the purpose of laundering money also had not been proved. Furthermore, the crimes of incitement of abuse of power and money laundering as put forward by the prosecutor in the particular case contained exactly the same elements. The Supreme Court ruled that in order to have a separate conviction for ML, an additional element showing the aim to conceal the proceeds of crime needed to be proved. The case, as per the decision of the Supreme Court was returned to the first instance court. This judgment appears to indicate, as far as self-laundering is concerned, the "aim to conceal" is a necessary element of the ML offence, and that simple acquisition or possession of proceeds of crime does not constitute ML. This has generated uncertainty as to the elements of the ML offence requiring proof (please see R3 for an analysis on this point).

209. As indicated above, the 2015 Supreme Court decision raised some concern among policy makers and practitioners as to how to interpret the ML offence and on its implications for investigations and prosecutions in the future (especially in relation to evidentiary requirements for proving ML and reaching a conviction). The assessment team considers that coordination and communication between the different State authorities in relation to the interpretation of this important judgment is lacking and should be strengthened, including through trainings of prosecutors and judges on evidential thresholds for establishing the underlying predicate criminality (if indeed this is a problem) and on whether the element of concealment is necessary where a suspect has used and acquired proceeds of crime, knowing that they are proceeds.

210. Due to the perception of high evidentiary thresholds described above, investigators and prosecutors have experienced difficulties in pursuing autonomous ML cases when the predicate criminality has been committed in country X ("country X typology")(see the analysis under IO2). In order to investigate these types of cases and file a criminal complaint for money laundering, Slovenian LEAs consider that they need to acquire evidence from FIU/LEAs of country X on the predicate offence. Given that the authorities from country X in most cases do not provide the required information or provide it late, it can occur, particularly when legal persons are concerned, that the Slovenian Financial Administration identifies tax irregularities (i.e. fake invoices) so that tax evasion can figure as the underlying predicate offence. This alternative path, however, cannot be used to pursue ML with a foreign predicate offence when the amount of tax which has been evaded is below 50,000 Euros.

211. Another obstacle which may hinder the proper prosecution/conviction of ML is related to the lack of resources of the judiciary (mainly in terms of administrative personnel) and judges' and prosecutors' insufficient expertise on financial forensics/crimes. While prosecutors can hire experts on financial crimes in individual cases, they do not have in-house expertise. This has been identified

by practitioners as an important shortcoming which would require priority action because it hampers pursuing ML and confiscation of assets.

212. Lastly, the authorities have not provided statistics on MLA. Nonetheless, they presented several examples of international cooperation demonstrating that they had proactively sought MLA from other States to support domestic investigations and prosecutions (see IO2).

Effectiveness, proportionality and dissuasiveness of sanctions

213. The sanctions provided by the CC for ML are set out in the TC annex (up to five years of imprisonment plus a fine and up to eight years plus a fine if committed in criminal association), are commensurate with other profit-generating crimes and have been assessed as being proportionate and dissuasive. The average custodial sentences which have been imposed by Courts have ranged between one year and two years and a half, thus are at the lower end of the "sanctioning" scale.

Table 13: **Type of sentence imposed following a conviction for a money laundering offence by a court of competent jurisdiction**

Year	Non custodial sentences			Custodial sentences			
	Fines (average in EUR)	Other than fines	Total number	Imposed prison sentence (average in months)	Suspended prison sentence (average in months)	Other measures	Total number
2010	-	-	-	-	-	-	-
2011	-	-	-	-	-	-	-
2012	6.291 EUR	730 hours of community service	1	11,5	9,3	0	5
2013	121.400 EUR	0	13	22	11,5	0	25
2014	6.165,9 EUR	0	9	31,5	16	0	13
2015	9.070,4 EUR	0	18	20	12,6	0	29
31.3.2016	-	-	-	12	20,5	0	5

214. Some of the authorities have also raised the concern that the statute of limitations which applies when a petition for an extraordinary legal remedy has been submitted is too short (two years).[50] For instance, the assessment team was informed of the existence of a high profile ML case related to a former domestic PEP for which the statute of the limitation period could expire in the near future.

[50] An extraordinary legal remedy is a proceeding through which a final court decision may be reversed in favour of the convicted person. Under Article 91(2) of the cc "If the final judgement in the proceeding for extraordinary legal remedy is annulled, the statute of limitations in the new trial shall be two years from the annulment of the final judgement".

215. As already noted only three cases involving liability of legal persons for ML were subject to court proceedings. In the above-mentioned cases the legal persons were sentenced with fines of only 35.000 Euros, which appears lenient based on the underlying predicate activity.

Extent to Which Other Criminal Justice Measures Are Applied Where the Conviction is not Possible

216. If during the pre-trial proceedings there are grounds for suspicion that a person possesses assets of illegal origin for a total value exceeding EUR 50,000 a financial investigation can be instigated in order to gather the evidence and information required for civil asset forfeiture. This has been elaborated in detail under the IO.8.

217. According to Article 498.a of the CPC, Courts can under certain circumstances confiscate money or property of unlawful origin for certain corruption related criminal offences even without a conviction. Nonetheless, there are concerns about the effective implementation of the confiscation regime in criminal proceedings given the low amounts of proceeds which have been confiscated in practice thus far (see IO8).

218. When pursuing ML in relation to tax offences committed abroad in a particular country, due to the high evidentiary requirements perceived by LEAs in relation to ML (see the analysis above) and the difficulties experienced in obtaining information on the tax predicate offence from the foreign counterparts, the Financial Administration has used its legal powers to identify the underlying predicate offence as tax evasion committed domestically. However this alternative path cannot be used to pursue ML with a foreign predicate offence when the amount of tax which has been evaded is below 50,000 Euros.

Overall Conclusions on Immediate Outcome 7

219. The authorities have made progress in securing ML convictions, including in relation to third-party ML as well as autonomous ML. Overall, however, the fight against ML activity is not fully prioritised and the number of ML investigations is low compared to the number of convictions for proceeds generating predicate offences. ML investigations and prosecution reflect to some extent the risks that the country faces, however, Slovenia's risk profile would warrant a higher number of ML investigations related to serious crime. Law enforcement Authorities and Practitioners, are faced with a number of obstacles in investigating, prosecuting and adjudicating ML cases, including in relation to evidentiary standards, the unresponsiveness of certain jurisdictions with regard to predicate offences committed in their territory and practitioners' insufficient expertise on financial crimes and forensics. The sentences which have been applied for ML appear to be at the lower end of the "sanctioning" scale and, as regards legal persons, are too lenient. Some criminal justice measures are applied when it is not possible to secure a ML conviction.

Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 7.

Immediate Outcome 8 (Confiscation)

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

220. The deprivation of proceeds of crime is one of LEAs' key policy objectives in Slovenia. The police have presented numerous documents confirming that confiscation is taken as a priority at the strategic and operational levels. The following documents identify confiscation as a priority at the strategic level and put an emphasis on financial investigations as a key component of combating proceeds generating crimes: '*Policy and Mandatory Instructions for Preparation of the Work Plan of Police 2017'; 'Resolution on National Program on Prevention and Combating Crime 2012-2016*; and '*Strategy on Controlling Economic Crime'*.

221. At the operational level the Police have developed specific guidelines on how to implement the respective laws. This includes guidelines with regard to both criminal and civil confiscation regimes, and guidelines on reporting to the Tax Administration and the Commission for the Prevention of Corruption on matters related to their portfolio in pursuing financial crimes. The State Prosecutor's

Office has defined its strategic goals in the Prosecution Policy document adopted in 2012.[51] The document prioritises, inter alia, the fight against economic crime (including ML) and, in parallel, the confiscation of criminally obtained assets. Prosecutors have also advised that at the strategic level a Working Group (set up in 2012 based on the Strategy of Controlling Economic Crime) has monitored, evaluated and coordinated the implementation of the *Decree on the cooperation of prosecutors, police and other institutions in the detection and prosecution of perpetrators of criminal offences and operation of specialised and joint investigation teams,* thus fostering the effective confiscation of proceeds of crime. As concerns the operational level, guidelines on civil forfeiture have been developed; however, at the time of the on-site visit similar guidelines had not been issued on confiscation in criminal proceedings.

222. In 2010, upon the initiative of their Director General, the Police have also created a working group at the national level which aims to improve the detection, investigation and prosecution of proceeds-generating crime and the confiscation of assets. The group's strategic goals are: i) to formulate and implement law enforcement activities so that money laundering investigations are prioritised and coordination, supervision and cooperation between the respective police directorates is ensured and improved; ii) to hold permanent training focusing on the detection and the prosecution of ML and predicate offences; iii) to improve the effective detection, confiscation and securing of proceeds of crime. The Group is operational and it regularly updates guidelines and instructions in the area of financial investigations and money laundering.

Confiscations of proceeds from foreign and domestic predicates, and proceeds located abroad

223. Slovenia has introduced both confiscation in criminal proceedings, which is mandatory under the Criminal Code (CC), and civil confiscation under the Forfeiture of Assets of Illegal Origin Act (hereinafter referred as 'FAIOA'). There are no limits as to the type and nature of property subject to confiscation.

224. Confiscation in criminal proceedings is limited to the property gained through the commission of the crime for which an indictment has been issued. The CC, following the 2012 amendments now provides a wide range of confiscation measures. Money, valuables and any other property gained through the commission of an offence must be confiscated ex officio. If the direct benefit cannot be confiscated, then property of equivalent value is subject to confiscation. Proceeds or property acquired or at the disposal of a criminal organisation is also subject to confiscation.

225. In practice, prosecutors mostly pursue, in the course of criminal proceedings, the assets deriving directly from the criminal offence(s) under scrutiny. In other words, alternative possibilities provided by the law (e.g. proceeds acquired or at the disposal of a criminal organisation) appear to be underused.

226. Financial investigations (as per the CPC) are to be carried out in parallel with criminal investigations. In practice, financial investigations are part of regular investigatory activities of the proceeds generating crimes. Consequently, the same investigators are in charge of pursuing the predicate offence(s) and the assets deriving from the offence(s). Although police officers receive regular training in this matter the level of expertise and persistency in pursuing parallel financial investigations still varies among different police units (see also paragraphs 194-195 under IO.7).

227. Financial investigations must be carried out whenever the criminal act of financing of terrorism is investigated (regardless of the amount of money or assets related to the specific criminal offence). However, the assessment team has not seen any such investigations so far (see under Immediate Outcome 9).

228. In the course of financial investigations, the police gather evidence related to the relevant criminal offence and to the proceeds of crime. It can seize the instrumentalities, the objects of the

[51] It should be noted that such policies are adopted upon designation of new Prosecutor General, so the new strategy is expected to be in place in May 2017.

criminal offence and any evidence. The interlocutors met onsite advised that although confiscation of instrumentalities is deemed to be a common practice, there have been cases where this principle has not been applied Police are not authorised to freeze or confiscate the proceeds of crime; they can, however, make suggestions to the state prosecutors to request such measures to court. Prosecutors are the only LEAs authorised to file such request to court. The court, if it finds the request reasonable, approves it in 2 - 3 days. Provisional measures may be ordered against the accused/the suspect, the recipient of the proceeds of crime or the third person who is the final 'beneficiary' of the proceeds. The order is for a duration of three months and can be prolonged. This measure can be imposed prior to the official launching of the investigation or prior to the filing of the criminal complaint and, in such cases, can last up to a maximum of one year. In the course of the investigation, the total duration of the provisional measure may not last more than two years. Once the criminal complaint has been filed and until the first instance proceeding has been finalised, the total duration of the provisional measure cannot exceed three years. Overall, from the time it is imposed up until the final court decision, the provisional measure may not last longer than ten years. The defendant is informed about the application of the provisional measure only once it has been ordered by the judge. The defendant can appeal the order but the appeal does not suspend the implementation of the measure.

229. The OMLP power to block the funds/postpone transactions is used by LEA to secure the assets before the court order is obtained. However, LEAs consider the 72h period as insufficient to gather enough evidence and obtain the court order. In addition, this OMLP power is available only for cases related to ML suspicion.

230. Nonetheless, LEAs frequently rely on this OMLP tool to secure the assets of the proceeds generating crime as most of them can easily be linked to ML. While this measure primarily serves to secure assets and prevent them from migrating (in terms of their whereabouts and provisional ownership), it is also applied in cases when the accused may use the assets (by him/herself or through a third person): to commit a crime or; to conceal, alienate, destroy or otherwise dispose of the assets in order to prevent or render substantially difficult their confiscation. The authorities have presented a case in which this measure has been applied.

Box 8: Case in which the OMLP's power to postpone the transaction was used

Case file 'Belgium'

In this case LEAs had identified the crime – an interned fraud (BEC-Business Email Corrupted). Assets had been generated through the above-mentioned crime which had been committed abroad against two companies.

In consultation with LEAs, the OMLP postponed all transactions on the account of the suspects without stating the upper limit of the assets. At that time, the balance on the bank account was 741,000 EUR.

While the postponement order was still in force, the OMLP was made aware of other transactions that concerned the afore-mentioned bank account. The transactions appeared to be related to the same criminal activity.

The prosecutor filed a motion to obtain a court order to freeze the assets, which was approved soon after by the judge. Three months after the freezing order was issued, the perpetrator of the crime had not yet been identified; the court decided to confiscate the assets (as per Article 498a of the CPC) and return them to the victims. The perpetrators of these internet frauds remained unknown.

However, the statistics provided by the authorities suggests that, although postponement orders were followed by freezing orders and investigations/prosecutions, the actual amount of confiscated assets following the application of these orders is modest.

Table 14: **FIU action and provisional measures**

Year	Number of postponement orders issued by FIU to suspend transactions/block account	Number of cases where the FIU order was followed by a preliminary investigation and a freezing order	Number of cases where a prosecution /indictment was initiated	Convictions and confiscation	
				Cases	Amount (in EUR)
2010	0	0	0	0	0
2011	1	1	1	0	0
2012	33	33	33	2	13,226
2013	14	14	14	0	0
2014	19	19	19	0	0
2015	9	9	9	0	0
31.3. 2016	3	3	3	-	-

231. Under Article 160a, Paragraph 2 of the CPC specialised investigative teams can be set-up for complex cases. The composition of the team primarily depends on the expertise needed for the particular investigation. In addition to the state prosecutor and the police, representatives of other agencies may be involved. All of the interlocutors interviewed on-site confirm that these teams so far have produced good results and have helped in building institutions' capacities to conduct/support complex investigations. Moreover, a similar platform of cooperation is also possible for civil confiscation purposes. Articles 13 and 14 of FAIOA lay down the rules on guiding the financial investigation and establishing a financial investigation team under the prosecutor's supervision and guidance.

Table 15: **Frozen, seized, confiscated and property recovered following conviction (years 2010 – 2016)**[52]

	Property frozen		Property seized		Property confiscated		Property recovered following conviction**	
	Cases	Amount (EUR)	Cases	Amount (EUR)	Cases	Amount (EUR)	Cases	Amount (EUR)
Conviction - based (as per CPC) regarding ML offences	58	77,603,697	4	1,231,650	12	2,274,274 and luxury car	18	6,334,115
Non-conviction - based (civil confiscation as per	23	37,302,259	4	75,430	3	2,176,574	n/a	n/a

[52] Conviction based refers to instances in which the order was applied as part of the sentencing for an underlying predicate offence. Conversely, non-conviction-based refers to confiscation executed following the civil proceedings as per FAOIO law.

FAOIO)*								
Total	**81**	**114,905, 956**	**8**	**1,307,080**	**15**	**4,450,848 and luxury car**	**18**	**6,334,115**
FT	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
* Data for 2015 and 2016 is not final **Order of restitution[53]								
*** Only for listed criminal offences as set in the FAOIO								

232. According to the statistics on the confiscation of assets deriving from ML (see the table above), between 2010 and 2016, 58 ML related cases ended up in 53 convictions[54]. Confiscation was executed in 30 out of 53 cases (12 by using the 'traditional' confiscation measures in criminal proceedings and 18 by using the order of restitution). The authorities have advised that in the remaining 23 cases no property was found as these were mostly self -laundering cases in which proceeds of the predicate offence were subject to confiscation.

233. The civil confiscation regime was introduced in 2011 under the FAIOA. Under FAIOA civil confiscation can be ordered if : 1) there is suspicion that a person has committed a crime as listed under Article 4 of the law (namely all profit generating crimes); 2) it is assumed that criminal assets are of 50,000 EUR value or more (this can be established e.g. during the house search or based on information from different data bases); 3) assets are not connected to a crime for which a conviction in criminal proceedings has been handed down. The State prosecutor may order a financial investigation against the person who was the subject of pre-trial or trial proceedings for having committed a criminal offence(s) as listed in the FAIOA. Civil confiscation can, therefore, be launched in parallel with the criminal proceedings and/or no later than i) one year following the acquittal/discontinuation of criminal proceedings or the dismissal of the criminal complaint; or ii) one year after the conviction became final. If this criteria is fulfilled a financial investigation team can be formed. In practice, once an investigator establishes (during the financial investigation which is a part of a criminal investigation) that the person possesses property in the amount of 50.000,00 EUR or more and if this property is likely to have been be gained through criminal activity other than the crime which is under investigation, then the investigator can propose to the competent prosecutor to initiate a financial investigation as per FAIOA. Reasonable doubt that the proceeds are of a criminal origin is the basis to initiate the financial investigation/civil confiscation proceeding. Prosecutors have advised that the reasonable doubt, in this context, means that the probability that the person under scrutiny is in a possession of illegally obtained assets is higher than 50%.

234. Given that most of the civil confiscation proceedings which have been initiated so far are pending before the Constitutional Court, there is no case law establishing clear standards and providing an interpretation of "reasonable doubt" – i.e. clarifying what probability means and what the applicable threshold to reach this percentage is. This ambiguity risks raising concerns among practitioners on how to apply the law in practice, and is likely to discourage them from proactively pursuing civil confiscation. Specific guidance on financial investigations under the FAIOA was issued

---

[53] Order of restitution is imposed as a part of a criminal sanction in cases when the assets or their equivalent could not be confiscated from the perpetrator or other recipient. In practice, this means that the perpetrator is obliged to pay (within the maximum of two years) an amount of money equivalent to the benefit made through committing the crime.

[54] The table above refers to 58 cases in total, indicating that, in addition to 53 convictions, 5 ML cases that have not yet been finalised were taken into account (for 'property frozen' and 'property seized' columns).

by the Prosecutor General in 2016. The document sets a methodology for the effective implementation of FAIOA and, inter alia, streamlines specific activities aimed at identifying and securing the assets, performing operational activities by the prosecutor before the financial investigation is launched, strengthening the cooperation with the Civil and Financial Departments of the Specialised State Prosecutor's Office and supervising the financial investigations.

235. Up until the end of the onsite visit, 30 financial investigations (against 116 natural persons and 76 legal persons) had been initiated based on FAIOA and with 13 investigations were in progress (against 40 natural persons and 1 legal person).

236. Statistics show that the Special State Prosecutors Office has undertook 20 financial investigations (based on FAIOA) against 88 natural and 75 legal persons – 10 of these investigations (against 34 natural persons and 1 legal person) have not yet been finalised; the District State Prosecutors Offices has initiated 10 financial investigations against 28 natural and 1 legal persons – 3 of those investigations (against 6 natural persons) have not yet been finalised. So far, freezing orders have been issued in 23 cases in the context of civil proceedings (either in the financial investigations or lawsuit phases), for a value of up to 37,302,259 EUR. Orders for the temporary forfeiture of assets have been issued in 4 cases for a total amounting to up to 75,430 EUR

237. By the end of the on-site visit, a total of 15 lawsuits had been filed for the forfeiture of assets of illegal origin (9 of them following the financial investigations ordered by Special State Prosecutor's Office and 6 of them based on financial investigations ordered by the District State Prosecutors Offices). Lawsuits had been filed against 32 natural persons and 7 legal persons for a total value of 22,236,864 EUR. However, only 2 judgments for forfeiture of assets of illegal origin in the value of 487,965 EUR become final. These judgments have not been appealed by the defendant through a constitutional complaint. The court has also granted one more lawsuit (in 2015) in which the forfeiture of assets of illegal origin was ordered for a value of 1,688,609 EUR. This judgement is, however, not final yet.

Box 9: Civil confiscation case

The head of a heroin trafficking criminal organisation was sentenced to imprisonment and proceeds of crime of approximately EUR 7,000 were confiscated. After the criminal procedure was over, the financial investigation based on FAIOA was initiated and, later on, extended to the wife of the perpetrator. A financial investigation team was established which included the participation of the police, the OMLP, customs and tax administration and was led and supervised by the prosecutor. It was established that the assets and expenditures of the offender exceeded his income by approximately 310,000 EUR. A lawsuit was brought against him in July 2013; the court of first instance (District Court on Ljubljana) delivered a decision in September 2014, establishing that assets were of an illegal origin and providing for their forfeiture in favour of the State. This decision became final with the decision of the Ljubljana Higher Court.

238. Other cases are pending before the Constitutional Court. The applicants – i.e. the defendants in the civil forfeiture trials - have submitted constitutional complaints based on the alleged interference of civil confiscation with the constitutional right to property and the absence of certain safeguards which are provided in criminal proceedings. Although civil confiscation is a civil procedure, the applicants claim that the features and specificities of this procedure, and of the law, in their *natura juridica*, are rather of a criminal nature. They have argued that certain investigative means used in the context of financial investigations by the investigative team and the prosecutors do not possess the necessary safeguards which defendants are guaranteed in the context of criminal proceedings. Apart from these individual complaints, two requests for review of the constitutionality of some specific parts of the law were filed by the Slovenian courts – Higher and District Courts of Ljubljana[55].

[55] The request of the Higher Court concerned the constitutionality of Article 5 in conjunction with Article 34; Article 27, Paragraph 3 and Article 10, Paragraph 5 of the FAIOA. This request was dismissed by the

While the assessment team has no mandate to discuss the matter of constitutionality and possible human rights implications of the aforementioned legal/judicial situation, the overall uncertainty and current status quo raises the concern as to whether the civil confiscation mechanism can complement confiscation in criminal proceedings.

239. While the inter-agency cooperation in financial investigations is considered to be successful, difficulties have been encountered in international cooperation with certain EU and non EU jurisdictions in information exchange and evidence gathering. This primarily concerns late responses or lack of a response to the requests submitted by the Slovenian authorities to their foreign counterparts. The requests mainly concern bank secrecy and beneficial ownership.

240. With regard to asset sharing, the Act on Cooperation in Criminal Matters with the Member States of the European Union serves as a basis for the country's policy in this context. The asset sharing depends on an agreement with the requesting state. If there is no agreement then the following rules apply:

- an amount of money which has been confiscated and does not exceed EUR 10,000 or the equivalent amount in another currency, is considered in its entirety revenue of the budget of the Republic of Slovenia. As concerns sums which exceed EUR 10,000 half of the sum is allocated to the Slovenian State budget and the other half to the ordering State;

- objects and property other than money are disposed of in one of the following ways, to be decided by a national court:

1) sold in accordance with national legislation; in this case, the proceeds of the sale are allocated in accordance with the preceding paragraph;

2) transferred to a competent authority of the ordering state; if the confiscation order covers an amount of money, the objects or property may only be transferred to the ordering state when that state has given consent;

3) disposed of in another way in accordance with national law if the preceding paragraphs cannot be applied.

241. With states which are not members of the European Union, the asset sharing is possible if so provided in ratified international documents.

242. As concerns assets repatriated from abroad, the prosecutors interviewed by the assessment team have referred to two on-going civil confiscation cases in which countries which do not have a civil confiscation regime (Austria and Croatia) were asked to temporarily secure assets. The request to freeze bank accounts which was addressed to Austria was based on the Warsaw Convention (CETS 198) while the request to Croatia was based on EU Regulation (1215/2012). The assessment team has not been informed of the outcome of these initiatives. Therefore, no finalised cases on asset sharing seem to be in place, while the authorities have not presented any case of asset sharing initiative with countries that are not EU member states. Such statistics suggest that these mechanisms have not frequently been applied in practice.

243. As already noted, the legislation does not limit the type and nature of the property which can be confiscated. However, practice shows that apart from money and real estate, property such as businesses and companies have almost never been the subject of confiscation. Problems have also been encountered in establishing property of an equivalent value in civil confiscation cases. As a matter of fact, there is no specialised officer with the expertise needed to properly estimate the value of the property. To illustrate this, an example was provided by the prosecutor. In an instance in which Rolex watches had been seized, the investigators in charge could not establish if their value was in the range of thousands of Euros or whether they were copies of an insignificant value.

Constitutional Court. On the other hand, upon request of the Higher Court, the Constitutional Court declared that some aspects of application of Article 4, Paragraph 1 of the FAIOA were not in line with the Constitution.

244. The most significant problem at the moment with regard to seized and confiscated property is the absence of a specialised asset management office. Currently, the seized and confiscated assets are held by the competent court. This solution does not appear to respond to emerging needs in relation to complex cases which involve complex property portfolio. The absence of such office may seriously hinder the effectiveness of the confiscation regime in general, and discourage investigators to pursue complex property such as businesses. Although the prosecutors have indicated certain initiatives by the Ministry of Justice aimed at setting up a specialised asset management office, no concrete/formal steps in this direction were communicated to the assessment team during the on-site visit. Overall, the assessment team was not convinced that with the current structure, maintaining the value of seized property and enforcing the courts confiscation orders can be effective.

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

245. Slovenia borders only with EU countries - Italy in the west, Austria in the north, Hungary in the northeast and Croatia in the south and southeast. The country has three international airports (in Ljubljana, Maribor and Portoroz) and one international harbour (in Koper).

246. For the transportation of cash and bearer negotiable instruments Slovenia has introduced a declaration system in line with the EU control system (see R.32 in the TC annex). Controls are in place at the international airports and sea harbours while the internal borders control is executed by the customs mobile units. Mobile units are part of the Customs investigations department, which belongs to the Supervision Department of the Financial Administration. These mobile units have the powers to search persons and vehicles and then report to the police any suspicion with regard to cash and BNI transportation. In addition, the units deal with under/overestimations of value of goods; tax rates; origin of goods: authenticity of documentation submitted for purposes of customs controls; referential rate; authenticity of invoice statements, etc. If customs officers detect non-declared/falsely declared cash, they report it to the Financial Administration and its special financial office responsible for penalties; and withhold the cash which is transferred to the national bank. These reports are automatically sent to the OMLP. However, no reports on ML/FT suspicions have been submitted so far. Although custom authorities deem that they have sufficient human resources, some additional equipment for detecting cash (e.g. X-ray devises and 'sniffing' dogs) would be helpful.

Table 16: **Reports filed on cross border transportation of currency and bearer negotiable instruments**

Year	Number of declarations or disclosures				Suspicious cross border incidents			Assets restrained (amount in EUR)	Assets confiscated (amount in EUR)
	Incoming		Outgoing						
	Currency	Bearer negotiable instruments	Currency	Bearer negotiable instruments	Suspicions of ML	Suspicions of FT	False declarations		
2010	**191**	**-**	**67**	**-**	**-**	**-**	**11**	**15,500**	**-**
2011	**177**	**-**	**90**	**-**	**-**	**-**	**19**	**8,000**	**-**
2012	**212**	**-**	**106**	**-**	**-**	**-**	**16**	**322,265**	**17,500**
2013	**99**	**-**	**43**	**-**	**-**	**-**	**2**	**0**	**8,000**
2014	**69**	**-**	**44**	**-**	**-**	**-**	**1**	**-**	**-**
2015	**99**	**-**	**33**	**-**	**-**	**-**	**0**	**-**	**-**

31.3.2016	-	-	-	-	-	-	-	-	-

247. Fines imposed for this category of offences are elaborated in the TC annex – R.32. No information on ML/FT investigation further to the detection of undeclared/falsely declared assets was provided to the assessment team. The authorities have also outlined that the overall cross-border flow has decreased since Croatia has entered the EU and border controls have been removed.

Box 10: Statistics on sanctions imposed

Year	Total number of cases in which a penalty is imposed	Total value in Euro of all the penalties imposed
2010	14	10800
2011	19	14500
2012	18	13500
2013	4	6500
2014	1	500
2015&2016 (up to 21/03/2016)	0	0

Consistency of confiscation results with ML/FT risks and national AML/CTF policies and priorities

248. The NRA, including its updated version of November 2016, dedicates a special chapter to the confiscation regime and the challenges it faces under 'National Vulnerabilities'. Nevertheless, the analysis is limited to the description of the legal framework and the specific amendments to the CPC which will enable provisional securing measures to last longer. More specifically, the Ministry of Justice has prepared an amendment to Article 502b of the CPC suggesting that the provisional measure in pre-criminal proceedings (after the investigation is launched) can last up to 6 months (instead of currently 3); once the indictment is in force it will last up to one year (instead of 6 months as it is currently the case); the total duration of the provisional measure (including all the prolongations) should be 2 years maximum (instead of 1 year as foreseen by the current legislation). However, in the absence of comprehensive statistics with a breakdown by types of predicate offences, an in-depth analysis on the effectiveness of the system is rather a difficult endeavour. Moreover, the NRA, including its updated version, has failed to analyse the effectiveness of the civil confiscation regime and the problems related to its implementation in practice; as well as the absence of a specialised asset management office responsible for seized and confiscated assets capable of maintaining their value and enforcing court confiscation orders. It appears that, while confiscation may be deemed by the authorities as a policy priority, a granular analysis with regard to specific risks was not conducted.

Overall Conclusions on Immediate Outcome 8

249. Slovenia has a sound legal and to a certain extent institutional framework in place (e.g. in the absence of an asset management office) to confiscate the proceeds of crime. However, there are some shortcomings as concerns its effective implementation.

250. It appears that there is a significant gap between the amounts of assets which have been frozen and those actually confiscated. When tracing the proceeds of crime, LEAs, in the absence of their own power to temporarily freeze assets, face difficulties in meeting the short deadlines provided under the law to gather the necessary evidence and in obtaining a court order for assets freezing. This process usually takes time, thus there is the risk that assets 'migrate', are dissipated or are no longer within the investigators' grasp. Furthermore, the validity of such court orders is very short.

Nevertheless, some positive developments have been noted in this connection. This primarily concerns the recent MoJ initiative to prolong the period of validity of freezing orders.

251. Furthermore, no special agency for managing seized and confiscated assets has been established. Consequently there is the risk that the value of seized and confiscated assets significantly decreases during the time they are held by the state. The system in place does not guarantee the effective management of complex assets such as businesses and companies.

252. With regard to offences committed outside of Slovenia, or when the proceeds are located abroad, no cases involving final confiscation were presented to the assessment team. On the other hand, there were several cases where proceeds have been frozen abroad upon the request of Slovenian LEAs. However, no detailed statistics have been provided on confiscation measures as a result of MLA or other type of international cooperation.

253. Last but not least, Slovenia faces difficulties in applying the civil confiscation regime. The issues of concern have been raised in the previous chapters of this Immediate Outcome.

254. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 8.**

CHAPTER 4. TERRORIST FINANCING AND FINANCING OF PROLIFERATION

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 9

1. Slovenia has an institutional framework in place to investigate and prosecute FT. LEAs and intelligence agencies are aware of current FT risks, pay due regard to suspicions of possible FT and make use of available (pre-)investigative methods. Annually, the police deal with five to ten cases that have certain indications of FT.

2. The authorities have not yet proceeded to formal investigations of FT, neither as a parallel financial investigation to terrorism nor as an independent offence. This was due to either not confirming the suspicions or lack of sufficient evidence.

3. Technical deficiencies in the FT criminalisation and uncertainty among practitioners about the need to prove a link to a terrorist act hinder the ability to properly investigate and prosecute all forms of FT.

Immediate Outcome 10

1. Slovenia relies on EU measures of implementation of UNSCR 1267 and subsequent resolutions, as well as EU implementation of UNSCR 1373, with some national complementing measures (primarily by establishing fines for violations of sanctions obligations). This reliance creates delays in implementation of UNSCR 1267. Although the ARM gives the Slovenian government powers to adopt national regulations transposing UN designations while awaiting EU implementation, these have not been used in practice.

2. Slovenia established a coordination group for the implementation of sanctions which includes all relevant stakeholders and provides a suitable platform for information exchange and cooperation between authorities with various spheres of competence. However, limited resources and infrequent meetings impede its full effectiveness.

3. Slovenia has not made any motions for designation of persons to the UN or EU lists, nor has it considered designations at the domestic level. No freezing of funds or other assets has taken place on the basis of the legal framework.

4. Authorities did not demonstrate adequate supervision of the implementation of TFS. Guidance provided to obliged entities is limited and not fully in line with standards. The authorities have not taken measures to publicize changes to listings when they occur. FIs met on-site demonstrated a basic level of awareness of the existence and the implementation of TFS. The representatives of the DNFBPs were generally unaware of the existence of TFS.

5. Authorities have made some efforts to assess the NPO sector and increase transparency in order to prevent abuse and misuse in the sector, but no in-depth assessment of their risks for FT abuse has taken place, and no risk-based approach to supervision of NPOs is in place.

6. LEAs and intelligence agencies demonstrated sufficient vigilance with regard to possible abuse of NPO sector for FT.

7. Despite limited governmental outreach, NPOs met on-site were in general aware of their obligations and possibility of abuse for illicit activities including FT.

Immediate Outcome 11

1. Slovenia mainly relies upon the EU framework for implementation of TFS concerning the UNSCRs against PF. This means that TFS in the field of PF are not implemented "without delay" with the exception of Iran. National powers to transpose UN designations before EU implementation have not been used in practice. In the case of Iran, sanctions were nevertheless implemented without delay as a result of the fact that the EU regime is more extensive than the UN regime. In the case of DPRK, the risk posed by delays is largely mitigated by the negligible trade and financial links between Slovenia and DPRK.

2. The Sanctions Coordination Group mentioned under IO.10 is responsible for coordinating all the sanction regimes, including proliferation related sanctions. Although it appears a useful platform for coordination and cooperation, the same concerns for its effective functioning exist as for IO.10.

3. FIs met on-site demonstrated a basic level of awareness of the existence and the implementation of different sanctions regimes, which would implicitly include those directed to PF. The DNFBP sector showed no awareness.

4. Authorities did not demonstrate adequate awareness and supervision of the implementation of UNSCRs relating to the combating of PF. The authorities have not systematically taken measures to publicize changes to listings when they occur.

Recommended Actions

Slovenia should:

Immediate Outcome 9

1. Urgently amend legislation to remedy identified gaps under R.5 in order to achieve full criminalisation of FT as required by the standard. To this effect, Slovenia is also encouraged to complete its ratification of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism as soon as possible.

2. Develop a national CTF strategy that sets out an appropriate approach to mitigate the emerging global, regional and national risks and clearly outlines the priority actions in the FT field.

3. Formalise the practice for conducting proactive parallel financial investigations in FT cases and continue to proactively follow up on any potential signs of FT identified both domestically and through international cooperation using – where relevant – formal investigation and prosecution of FT.

Immediate Outcomes 10 and 11

1. Provide adequate human resources for the work of the Sanctions Coordination Group, in particular the MFA, to effectively coordinate the implementation of FT and PF sanctions.

2. Ensure that TFS are implemented without delay. This can be done for example through the effective use of national powers to implement UNSCR 1267 before the transposition to the EU framework.

3. Provide adequate training to supervisory authorities regarding the implementation of the FT and PF sanctions; ensure adequate supervision regarding the implementation of the FT and PF sanctions and collect relevant statistics on those supervisions and measures imposed.

4. Conduct outreach activities to reporting entities in order to raise awareness on implementation of FT and PF sanctions, especially among small- and medium-sized reporting entities and DNFBPs as awareness was lowest in these sectors; and establish a more proactive system to promptly notify reporting entities of new listings.

5. Conduct an in-depth risk assessment of the NPO sector, with involvement of all relevant stakeholders, to identify those NPOs most at risk for FT, and ensure that the risk-based approach to supervision of NPOs is in place.

6. Conduct targeted outreach activities to the NPO sector regarding the prevention of potential FT abuse.

255. The relevant Immediate Outcomes considered and assessed in this chapter are IO.9-11. The recommendations relevant for the assessment of effectiveness under this section are R.5-8.

Immediate Outcome 9 (TF investigation and prosecution)

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

256. There have been no prosecutions or convictions for FT in Slovenia so far.

257. Slovenia has incorporated in its NRAs a very limited analysis of threats related to FT (see IO.1). Based on an analysis of the institutional, policy and operational structures and cooperation and information flows at the domestic and international level, this threat was estimated to be at 'Low' level.

258. The analyses of national and sectorial vulnerabilities in the NRAs were very much targeted at the potential for ML abuse, and the potential for abuse of certain activities or products for FT has not been taken into account. One case where this is particularly notable relates to payment institutions. It is not explored whether their operations (with the use of both banks and private companies as agents) are vulnerable to FT, in spite of international awareness about this possibility[56] and domestic awareness of their potential use as FT channels among authorities interviewed on-site. An exception to the lack of FT specific findings in the NRAs is the consideration of banking sector vulnerabilities in the updated version. It is noted in this context that banks have faced new risks in the 2014-2015 period related to verifying customers' identity in case of migrants without personal documents. An even bigger problem observed for the banking sector in the updated NRA lies in the sector's ability to detect possible cases of FT, as banks reportedly do not have experience in this field and are not provided with sufficient guidance.

259. A formal in-depth country-level assessment on FT risks has thus not been conducted. The overall understanding of FT risks was found to vary between the different stakeholders interviewed on-site. Nevertheless, the evaluation team found during the on-site visit that understanding of risks related to FT among LEAs and intelligence bodies is satisfactory.

260. According to the authorities, FT issues may be considered on a case-by-case basis in the context of regular terrorism risk assessments which are made by the mixed counter-terrorism working group operating under the National Security Council. This working group is composed of various competent authorities including LEA and intelligence bodies (see further under core issue 9.3 –

[56] www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

'National strategies'). These assessments are classified information and their findings are not shared with institutions outside of the working group, let alone the private sector.

261. It is the view of these authorities that the direct FT threat for Slovenia can be assessed as low but that recent developments related to ISIS and other terrorist groups in Syria and Iraq have increased the risks and warrant high vigilance. In their understanding, the most significant emerging threats are support by local NPOs of international fundamentalist religious terrorism, exploitation by terrorists of recent migration developments and support of Slovenian citizens travelling to conflict zones abroad to join foreign terrorist groups. The authorities believe that so far, ten persons (including a big family) have travelled from Slovenia to Syria. It was confirmed for three of them that they have stayed in territory controlled by ISIS. One of the three reportedly died; two others came back of whom one was extradited to Italy based on suspicion of involvement in recruitment activities; and the other was convicted in Slovenia for possession of illegal firearms (see further under core issue 9.5).

262. As main vulnerabilities, the authorities consider money flows in cash which can easily go undetected and money flows through payment institutions. The authorities also consider vulnerable the geographical location of Slovenia between the Western Balkans, close to countries with high numbers of departing and returning foreign terrorist fighters, and close to other EU countries, where large terrorist attacks have recently been executed. Two persons arrested in Austria who are suspected to be accomplices in the attacks in Paris in November 2015 briefly crossed Slovenia, hiding in the refugee movements. The authorities note that, nevertheless, almost all requests for foreign cooperation since the recent attacks in Europe have been related to terrorism and not specifically to FT. Requests for information related to FT were more common 10 to 15 years ago, when many activities were observed in the Balkan region relating to fundamentalist Islamist NGOs with financing flows from other regions.

263. In light of the nature of current emerging risks, it is an important positive development that Slovenia has signed the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism at the occasion of the International Conference on Foreign Terrorist Fighters in Riga in October 2015. In order to proceed with ratification, the Ministry of Justice of the Republic of Slovenia has been preparing the necessary amendments to the Criminal Code, which will include the incrimination of financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training. At the time of the on-site visit, the institutional consultation phase was in its final stage.[57]

264. It appears that the awareness among key institutions about new emerging risks has not been translated to broad country-level action to adapt the private sector to these risks. Both supervisors and reporting entities indicated that they are in need of more information on how to detect suspicious activity potentially related to FT. Ultimately, the lack of understanding among reporting entities could negatively impact on the understanding among authorities, as indicators may go unnoticed and may not come to the attention of authorities. There have been some positive examples of information flowing from the private sector to authorities on potential FT. Some outreach activities have been undertaken, in the form of recent trainings for the banking sector with a focus on FT and dissemination of the FATF report on FT indicators for reporting entities. However, in general, as noted under IO.1, the evaluation team was concerned about the low level of awareness on FT risks among many representatives of reporting entities met on-site, which can be a vulnerability of the system in itself.

TF identification and investigation

[57] Authorities have advised subsequently (April 2017) that the relevant Law on Amendments to the Criminal Code is in the legislative procedure and that the National Assembly will debate it during its May 2017 session.

265. In Slovenia, there are three governmental bodies with special units in place to combat terrorism – the Slovenian Intelligence and Security Agency (SISA), the Intelligence and Security Service of the Ministry of Defence (ISS) and the Police. Within the General Police Directorate at state level, the Counterterrorism and Extreme Violence Section operates as part of the Organised Crime Division with five senior criminal police inspectors specialised for CT issues. At regional level, there are eight Police Directorates with Organised Crime Sections, with in total 28 specialists for CT. No additional resources have been allocated in recent years. Within SISA, there is a unit for CT, proliferation and organized crime.

266. All three bodies cooperate on the basis of respective legislation and bilateral agreements. At operational level there are regular contacts between their representatives, performed within a special tripartite working group which enables close cooperation. Through regular working meetings and official documents related to on-going cases, the tasks of the bodies involved are defined and data and findings are exchanged. This structure also enables the parties to include other relevant competent authorities where necessary. The evaluation team had the impression on-site that relevant information, including from foreign counterparts and in case of possible matches with international FT sanctions lists, flows regularly between these stakeholders as well as with the OMLP.

267. Annually, the police deal with five to ten cases that have certain signs of FT and correspond to individual indicators, in the pre-investigative phase. The information is acquired through operational work of the police; on the basis of findings of the OMLP; within the framework of criminal intelligence work; or through international cooperation. According to the statistics provided to the assessment team, obliged entities have filed 5 STRs related to FT to the OMLP in the year 2011, 6 in 2013, 1 in 2014, 5 in 2015 and 1 in 2016 (all by banks). From foreign FIUs, the OMLP has received 1 report in 2011, 2 in 2015 and 1 in 2016 on FT which it treated as an STR in order to collect data and provide answers to the requests for information. The OMLP sends all information related to FT that it receives from reporting entities or foreign counterparts to the Police. There are also statistics on police-initiated STRs, where the Police requested more information from the OMLP related to potential FT: 1 STR for each year since 2010, except for 2011 and 2016 (up until November). There are no statistics on requests to the OMLP received from SISA but as noted above, interviews on-site confirmed the exchange of information.

268. The verification of information by the police takes place mostly at the regional level in cooperation with the Specialised Office of the State Prosecutor, which is responsible for the prosecution of the perpetrators of criminal offences which require special qualifications and organisation of state prosecutors and a higher level of efficiency. No case of FT suspicion has been confirmed in Slovenia so far and no criminal complaints on FT have been filed with the competent prosecutor's office with a view to indicting a perpetrator.

269. As follows from the cases explained to the assessment team, authorities generally pay due regard to suspicions of possible FT, both on the basis of independent information on financial flows and in parallel to (pre-)investigations into other suspected terrorist activities (recruitment, incitement). Bank transactions, money remittances, and other evidence that could suggest financial links are checked as standard procedure, although there are no operational manuals in place to prescribe that. In the stage of investigating, evaluating and acquiring information, the SISA and ISS are included, in accordance with the Tripartite Agreement, and the various investigative techniques that the respective LEAs and intelligence bodies have at their disposal are used in coordination. The OMLP and tax authorities are also involved in relevant checks on funding flows. International cooperation with foreign law enforcement and intelligence agencies, mostly through informal channels, is actively sought and provided. Such checks have taken place in the contexts of suspected foreign terrorist fighter travel to Syria (see Box 11), suspicion of exploitation of the migrant movements by terrorists, and potential abuse of NPOs to fund fundamentalist activities.

Box 11 – Foreign terrorist fighters

Two pre-trial procedures relating to foreign terrorist fighting have been applied in Slovenia.

In the first of these procedures, a Slovenian citizen has been surrendered to Italy on suspicion of commitment of the offence of recruitment of foreign terrorist fighters, on the basis of the European detention order. Besides the cooperation with Italy, Slovenian prosecutors have also made a formal request for international legal assistance to foreign authorities (Bosnia and Herzegovina) within the investigation, with intent to collect evidence. Two coordination meetings were arranged at Eurojust between representatives of the Slovenian Specialized Prosecutor's Office and representatives from the Italian police and prosecution service and representatives of the Prosecutor's Office of Bosnia and Herzegovina.

The second proceeding concerns a Slovene citizen who returned to Slovenia after a short stay in Syria. Based on cooperation with foreign intelligence partners and previously gathered information, a house search was conducted during which firearms and munition were found and seized. At the direction of the competent Public Prosecutor's Office, the Police continues with the gathering of information, primarily with the objective of confirmation of active involvement of the citizen in execution of violence against civilians or fighting on the side of terrorist organisations, for which criminal complaints could be filed.

Within the investigations, the Slovenian police cooperated with the OMLP in reviewing financial flows of involved persons. These checks did not reveal the existence of external financing sources.

270. Authorities indicated that there is no threshold for volume of transactions that are investigated, because they are aware that terrorism can be funded with low amounts of money. Some examples were given where LEAs and intelligence followed also minor money flows to check indications for FT. Nevertheless, the evaluators have concerns as to whether this approach is systematically understood and applied, since some representatives also seemed to suggest that when sums involved are particularly low, it is 'obvious' that persons are not financed by third parties.

271. Up to the time of the on-site visit, the (pre-)investigations discussed above have not resulted in criminal prosecutions due to either lack of evidence or not confirming the suspicions. While in the latter cases it is understood that the investigated activity appeared to be legal (see case example in Box 12), the evaluators have some concerns regarding the cases related to terrorism and terrorist financing where formal investigations or prosecutions were not pursued due to the lack of sufficient evidence. It appears that there is perception among the practitioners that the required level of proof to raise the suspicion of terrorist (financing) activities to a sufficient level in order to proceed to formal investigative stage is particularly high, in spite of the fact that the level of proof in criminal procedure is formally the same for all offences. Practitioners further made reference to a case from 2015 wherean Italian citizen (chemist by profession) used the post office in Slovenia to send chemicals to Czech politicians. In this case it was decided to prosecute him in Slovenia and charge him for terrorism and extortion, but in 2016 the case failed, reportedly due to failure to prove the intent to commit the terrorist crime.

272. Difficulties to raise FT suspicions to a sufficient level to pursue cases also relate to the technical deficiencies in the FT offence which may have an adverse impact on FT investigations (see also R.5). The necessity to prove direct intent and particular purpose of the financier toward terrorist activity is most crucial in this regard. In the absence of jurisprudence, prosecutorial and judicial authorities were furthermore not unequivocal in their opinion about whether a link between the funds and a specific terrorist activity would need to be proven based on the text of the FT offence. When an individual intentionally gives financial support to a known terrorist organisation, there is possibility that this may be sufficient to fulfil the elements of the offence regardless of the subsequent use of the funds according to the opinion of most of them, as it is the intent at the moment of payment which counts. However authorities indicated that if there was a "legitimate" purpose for the money transfer it is doubtful whether it may constitute FT. Funding of individual terrorists (including foreign terrorist fighters) in the absence of a link to a specific act might be particularly hard to pursue under current legislation.

273. The gaps in the FT offence could also impact on the possibility of Slovenia to provide effective international cooperation in the CFT field. Requirements for dual criminality vary between different legal bases that can be used for international cooperation (see R.37), but for coercive measures with non-EU countries, dual criminality is considered a pre-condition for execution of requests. Judicial authorities met on-site confirmed that they would not automatically conclude that a lack of exact consistency between Slovenian and foreign law would be a reason to reject an MLA request. However, they would hesitate to approve execution of a request if the requesting state criminalizes FT much broader than Slovenia. This has so far been a hypothetical question, but there could be an adverse impact in the future.

274. The policy-making authorities (MoJ) are taking action to try to improve the situation. The Ministry of Justice advised that the planned Law on Amendments to the Criminal Code, which should enable ratification of the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, includes relevant amendments to the FT offence and related terrorist offences. They have indicated that it was tried twice in the past (in 2004 and 2012) to amend the legislation in order to clearly broaden the scope of the offence. The amendments failed due to opinions that they would be contrary to principles of fundamental law.

Box 12: FT suspicions not confirmed

The OMLP informed the Police about a possible criminal offence of FT. According to the OMLP's report, certain individuals had received several money transfers amounting from 1,000 to 2,000 EUR from natural persons in three countries in Europe and Africa through money transfer systems.

After a thorough examination of the report and based on the information collected in interviews, the Police established that the suspected persons had business transactions with a person residing in a Western European country whose company was involved in the purchase and transport of vehicles for the African market. The money that they received through the money transfer systems was meant for the seller in Slovenia as payment for the vehicles, plus some profit for carrying out the purchase, transfer of property and transport of the vehicles from Ljubljana to the European country where the company was based.

The OMLP checked all the bank accounts related to this case; and further data was collected from the tax authorities, banks, customs office, and the Business Register. Through the collection of data, the police officers established that in this case, the activities were legal. Since the collected data did not give grounds for a crime report, the criminal police officers sent a report to the District State Prosecutor's Office pursuant to the provisions of paragraph 10 of Art. 148 CPC.

TF investigation integrated with – and supportive of – national strategies

275. There are no national strategies in place in Slovenia which focus specifically on terrorism or FT. Terrorist criminal offences which include FT are included in the Resolution on National Programme on the Prevention and Combating of Crime 2012-2016 as one of the key threats to public safety that need effective actions of competent authorities in the domestic and EU framework (see also IO.1). At the time of the on-site visit, authorities were in the process of preparing the new Resolution for 2017-2022 but no information was available to the evaluation team on the consideration that FT will receive in this strategic document. The National Security Strategy of the Republic of Slovenia (last version adopted by Parliament in 2010), chapter 6.3 Organized Crime and combating terrorism, also recognizes the threat of terrorism, with its corresponding forms of extreme violence, as one of the significant threats, but again it did not become clear whether FT receives particular attention.

276. Based on the National Security Strategy, the National Security Council has been established: a government advisory and coordinating body responsible for the national security policy and direction of its goals. A mixed working group for combating terrorism operates within the Council which organises the CT activities of authorities at the strategic level. The mixed working group includes high-level representatives from the Police, intelligence agencies SISA and ISS, the Slovenian army, the OMLP, FARS, MoJ and MFA. The Group regularly makes an updated classified terrorist

threat assessment for top-level political decision-makers, which may include FT issues on a case-by-case basis. Operational information from the participating authorities gathered within their spheres of competences feeds into this assessment.

277. A national strategy on prevention and combating terrorism is yet to be adopted even though its adoption was already foreseen in the National Security Strategy of 2010. According to the competent authorities (Police), the draft Strategy on prevention and combating terrorism is currently in procedure of consideration. It defines FT as one of the priorities and sets out also the connections between terrorism and organized crime which mostly present exploitation of criminal logistical support methods and financing. The draft of the strategy also highlights that special attention must be devoted to the potential abuse of NPOs and other legal entities which could conduct FT activities.

278. As regards the specialization of authorities, as noted above there are special units in place for CT within the LEAs and intelligence bodies which appeared sufficiently vigilant and knowledgeable with respect to FT. Verification of information by the Police takes place in cooperation with the Specialised Office of the State Prosecutor, responsible for the prosecution of complex criminal offences including FT. The Specialised Office was established in 2011 and its resources were strengthened in 2014, in line with strategic documents outlining the fight against complex crime as a priority in Slovenia (see IO.1).

279. Furthermore, the Slovenian police has organised since 2004 a specialised action called OKLEP which includes police units at the national, regional and local levels. In this framework, regular periodic training (at least twice a year) takes place to transfer good practices and knowledge on new modus operandi, acquired by senior police officials as results of participation in working groups, international training and investigations, to other police officers. The trainings are prepared and organised by the Senior Criminal Police Inspectors Specialist for CT at the state level. One of OKLEP's objectives is to 'train the trainers' in order to make the recipients of the trainings spread the acquired knowledge further at the regional and local level. So far approximately 700 police officers were trained from different organisations (border police, local stations, regional level, special units).

Effectiveness, proportionality and dissuasiveness of sanctions

280. No sanctions or measures have yet been applied for FT.

281. As described in the TC Annex, available sanctions for natural persons and legal persons appear sufficiently proportionate and dissuasive. According to Art. 109 CC natural persons convicted of FT are subject to imprisonment from one to ten years. A more severe penalty is prescribed if an offence was committed within a terrorist organisation or group to commit terrorist acts, in which case imprisonment between three and fifteen years is foreseen. Under the Liability of Legal Persons for Criminal Offences Act, sanctions that may be imposed on legal persons liable for a FT offence are: fine (50,000 – 1,000,000 EUR), confiscation of property (half or more of the legal person's entire property), winding-up of legal person and prohibition of disposing with securities held by the legal person.

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

282. Even where investigative activities did not confirm suspicions of FT, useful findings and information obtained are inserted into the system of operational information. Persons of interest can afterwards still be subject to monitoring and gathering of further information in the context of (criminal) intelligence work. In case of some specific findings, information is also forwarded to Europol databases (FP Travelers, EIS).

Box 13: Preventive interview

The evaluation team was informed about one case where a Slovenian citizen organised the collection of funds to help Syrian citizens. As the initial findings did not confirm a criminal offence, a preventive interview aimed at awareness-raising was conducted by the police. The individual was warned that the manner in which he forwarded the funds posed FT risks. He was advised to contact well-established international organisations collecting assistance for Syria if he wished to provide relief.

283. Although it has not happened yet for FT, it appears from examples provided to the evaluation team that prosecutorial authorities are willing to pursue other criminal sanctions outside of the terrorist sphere if they are of the opinion that high standards of proof would decrease the likelihood of obtaining a successful conviction for a terrorist offence.

284. From a broader perspective, it must be noted that Slovenia has shown a proactive approach to developing and implementing measures to recognise, detect and prevent violent radicalisation. Slovenia dedicates special attention to the harmonization of its strategic policies with the EU counter-terrorism strategy and EU strategy for combating radicalization and recruitment to terrorism. The Police and the Ministry of Health have been cooperating in this field for more than two years. Within the EU Radicalisation Awareness Network, the Slovenian Police has set up a national RAN platform upon resolution of the National Security Council. Through the platform, training on (de-)radicalisation has been organised for participants from various areas (e.g. health care, schools, social care, NGOs, local and religious communities).

285. Slovenia has also taken an active role in EU-level initiatives to spread the preventive approach to third countries.[58] In particular, it is active within the Western Balkan Counter Terrorism Initiative, which includes political, strategic and operational level activities. At the operational level, the authorities advised that CT police and intelligence structures from Western Balkan and EU countries from the region (Austria, Croatia, Czech Republic & Slovenia) have defined the strengthening of mutual cooperation in timely detection and prevention of FT as one of the priorities in their 2016-2017 plan of activities.

Overall Conclusions on Immediate Outcome 9

286. The evaluation team shares the view of authorities that FT risks in Slovenia are relatively low, but that possibilities for FT activity cannot be neglected and should be dealt with vigilantly, in light of established vulnerabilities and current emerging international and regional threats.

287. In the absence of prosecutions and convictions for FT, the judgment of the evaluation team should be based on the appropriateness of the institutional framework in place to investigate the financial aspect of terrorist activities when necessary. It is concluded that Slovenia adopts a proactive, coordinated approach against terrorism, including FT. This approach is based mainly on the intelligence work of special divisions within the SISA and the Police and with support from the OMLP and other partners when necessary.

288. Nevertheless, the gaps in the FT offence appear to have negative repercussions on the abilities of authorities to effectively pursue FT and must be remedied urgently. Furthermore, the lack of communication to the private sector on FT risks and the lack of a national strategy for FT are believed to weaken the authorities' ability to effectively pursue FT.

289. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 9.**

Immediate Outcome 10 (TF preventive measures and financial sanctions)

Implementation of targeted financial sanctions for TF without delay

290. Slovenia mostly relies on EU measures of implementation of UNSCR 1267 and subsequent resolutions, as well as the EU implementation of UNSCR 1373, with some national complementing measures (primarily by establishing fines for violations of sanctions obligations in domestic regulations).

291. Targeted financial sanctions (TFS) under UNSCR 1267 and subsequent resolutions are not implemented in a way that complies with the FATF Recommendations. The EU's transposition

[58] See for example: NOTE from EU Counter-Terrorism Coordinator to Council, Foreign Fighters and returnees: Implementation of the measures decided by the JHA Council on 9-10 October 2014, www.statewatch.org/news/2014/nov/eu-foreign-fighters-16002-14.pdf .

system is too slow to ensure that assets are frozen without delay and no Slovenian measure compensates for this. A delay occurs between the date of a designation by the UN Committees and the date of its transposition into European law. This arises because an EU legal act can only enter into force after translation into 24 European languages and publication in the EU Official Journal. An expedited procedure has recently been adopted by the European Commission for transposition of new listings by the 1267/1989 (Al Qaida) Committee under EU Regulation 881/2002. This procedure ensures that new listings come into effect faster. Consequently, the gap between publication of new designations by the UN and EU transposition has closed from 7-29 days in 2013 to approximately 4-12 working days of the UN decision in 2015 and 3-9 working days in 2016. This is an important improvement but still not fully consistent with the requirement to implement sanctions without delay. Furthermore, the transposition of 2 designations by the 1988 (Taliban) Committee in 2015 (up to late November) still took 15 and 127 days respectively.

292. These delays cast doubt on the ability of the authorities to freeze rapidly the assets of persons or entities targeted by the UN, and have a negative impact on the effectiveness of action by the Slovenian authorities.

293. The authorities have advised that the APMLFT could be used to bridge gaps between the UN and EU designation, should the need arise. Under the APMLFT, the OMLP has the power to temporarily suspend transactions on its own initiative or upon request of foreign counterparts in case of reasonable suspicion of FT (Art. 96, 110). The length of this suspension was recently extended from 72 hours to 3 working days. LEAs could then also apply for a court order for further temporary freezing on the basis of the CPC. However, the evaluation team emphasizes that these measures are not fit to ensure a full implementation of TFS obligations.

294. The basic domestic legal act governing the field of TFS in Slovenia is the Act on Restrictive Measures (ARM, in force since 2006). On the basis of this act, the Government established the Sanctions Coordination Group (SCG) with a purpose of monitoring and coordinating the implementation of all international sanctions regimes that are binding on Slovenia and other restrictive measures which Slovenia can choose to introduce domestically. The SCG is chaired by the MFA and composed of representatives of various Ministries including the Ministry of Finance, Ministry of Interior and Ministry of Justice, the BoS, the FARS, the SISA, the Nuclear Safety Administration, and the OMLP. It appeared from the on-site interviews with authorities who are members of the Group that they were well aware of the group's purposes and division of responsibilities, but that they did not fully gauge the importance of its work.

295. The SCG does not meet regularly, but practices written procedures in reaching common positions. The functioning of the Group is governed by internal Rules of Procedure. On 26 October 2016, the Group adopted an Annex to these Rules. The Annex elaborates internal mechanisms for the group for proposing and considering designations at the national level (see also under R.6). According to this Annex, the SCG can consider to submit a proposal for national designation to the Government upon motion of the Group members, EU member states or third states. The adoption of more detailed provisions on domestic designations is a welcome development, but their effective use could not yet be demonstrated given the short period that has passed since their adoption. Prior to the Annex' adoption, the legal framework (formed by the ARM, the Act Establishing the SCG and the Rules of Procedure) was silent on exact designation procedures although ARM did introduce the broad legal power to adopt domestic targeted sanctions already in 2006. It appears that the information about the new mechanisms has not yet been made known to other states, as the Annex is an internal, confidential document. No designation proposals for TFS in the field of FT have ever been made within or to the Group.

296. The evaluators have some concerns about the sufficiency of resources available to the members of the Group, in particular the MFA, to effectively coordinate the implementation of TFS. The issue of resources is exacerbated by the fact that the ARM only provides a basic legal framework for international restrictive measures, and that for each sanction regime separate detailed implementing regulations need to be drafted. This poses a heavy regulatory burden on the MFA.

297. Furthermore, it became clear from the on-site interviews that there is a clear need for more governmental-level support to the private sector for the implementation of sanctions. The authorities do not systematically publicize or communicate changes in listings to the private sector each time they occur. The assessors were informed by the representatives of financial institutions that it takes long to obtain answers from the MFA. In the absence of effective action of authorities, the private sector (Banking Association) took it on itself to launch initiatives to improve the implementation of TFS, including the issuance of sector-specific guidance, for which the MFA was consulted and provided comments.

298. The MFA provides general guidelines for the implementation of TFS on its website. The SCG recently updated them on 26 October 2016. However, at the time of the on-site visit, the updated version was not yet made available to interested parties on the MFA's website. The guidelines are not fully in line with the standards regarding the required timing of freezing, as they advise financial institutions to inform and await an answer from the MFA in case of a suspected match, before freezing funds that are potentially linked to a listed entity (see R.6). However, in case when all identifiers are met and there is no doubt, according to the guidelines, the freezing takes place immediately. Moreover, interviews with banks on-site nonetheless indicated that this deficiency has not withheld them from blocking funds *before and until* getting an answer in cases of potential matches.

299. The banking supervisor is well aware of its competences under the ARM and the domestic regulations complementing the EU legal acts to supervise the implementation of sanctions within banks. This is checked within AML/CFT supervision. According to the BoS, no irregularities have been identified so far. The BoS detected a need for further guidance to banks on gathering of information on senders of payments which are not their customers, in order to determine matches with the lists, and is preparing further guidelines in this area. For other supervisors, including those for financial institutions, supervisory competences for TFS under the relevant legal framework are not so clear (see R.6) and awareness was generally low.

300. Sporadically over the past years, trainings have been organised for the banking sector by the OMLP in cooperation with the Banking Association, which included TFS as a topic and in which the MFA representative participated. It appears that most financial institutions would be ready to contact the OMLP or MFA in case they need advice on implementation of TFS or in case of a potential match.

301. FIs met on-site (with the exception of currency exchange offices) demonstrated a fairly high level of awareness of the existence and the implementation of TFS. The same cannot be stated for the representatives of the DNFBP sector where awareness was often completely lacking. Real estate agents and lawyers met on-site claimed that they could rely on the checks by banks, because they would work only with clients who have a bank account in the EU (lawyers) or because all transactions would take place from bank accounts (real estate agents).

302. Most FIs met on-site confirmed to have integrated sanctions lists in their customer screening and monitoring processes. According to the BoS, all banks but one small savings bank have an IT-system which integrates sanctions lists. However, the evaluation team still has concerns over timeliness and depth of checks. In some FIs, screening of existing clients only takes place periodically (e.g. once a week or once a month) which impacts on their abilities to implement TFS without delay. Furthermore, if the data on beneficial owners is kept in paper form, and there are such cases in practice, then it is impossible to automatically cross-check beneficial owners against the sanctions lists. Understanding of beneficial ownership in FIs also does not always extend to indirect ownership (and with exception of the banks, understanding also often did not cover managers or directors of companies). These gaps in the screening of beneficial owners, coupled with a lack of understanding of the required scope of application of the sanctions, negatively impact on efforts to identify funds that are owned or controlled indirectly by listed entities. Only one bank reportedly uses a group-wide list of entities linked to UN designated persons.

303. Slovenia has not made any motions for designation of persons to the UN or EU lists. For EU lists, the competent authority in Slovenia for submitting designation proposals to the Council is the MFA, which has a representative in the CP 931 Working Party (WP) responsible for designations. So far, Slovenia has not made such a motion, but when designations from other member states are considered in the CP 931 WP, group members of the SCG can provide input for the position to be taken by the Slovenian government. From interviews with SCG members and from the recently adopted Annex to its Rules of Procedure it further became apparent that, should a situation arise in which competent authorities want to propose a designation to the UN, the MFA would take the lead in preparing such motions and would be supplied with information by other SCG members that they can gather in their spheres of competence. The final decision-maker would be the Government upon proposal of the SCG.

Focused and appropriate measures to NPOs identified as vulnerable to TF abuse

304. There are three main legal forms in which non-profit organisations (NPOs) operate in Slovenia, namely associations, institutes and foundations. The most common type of NPOs in Slovenia are associations (including federation of associations) which take a portion of 72% of the total number of NPOs. However, most of the financial resources of the sector are held by the institutes, trade unions and religious communities. Most associations are formed for sports and recreational activities, to provide assistance to people, for cultural and artistic activities or for scientific research and education. For more information on the various legal forms of NPOs see R.8.

305. Slovenia demonstrated a strong capacity to obtain information on its NPO sector, at least as far as associations, institutes and foundations are concerned. They must be registered with public bodies, which keep data on the registered NPOs and provide this upon request to the general public or other public authorities. Authorities have informed that in 2015-2016, there were 112 of such requests. Part of the data is also transmitted to the public register for legal persons (Business Register), meaning that it can be easily checked by anyone on-line. Some minor gaps in the available information are described under R.8.

306. The Centre for Information Service, Cooperation and Development of NGOs (hereinafter – the CISCD; an umbrella organisation of NPOs) also holds comprehensive statistics on the whole NPO sector, including on sources of funding. One quarter to one third of the total income of NPOs stems from grants from the budget and other public funds. The government applies extensive oversight to the NPOs which receive public funding. Especially associations with a special 'humanitarian' status, which can distribute funds untaxed to individuals for humanitarian purposes, are subject to strict obligations for obtaining funding and justifying expenditures. The Office for NGOs within the Ministry of Public Administration has defined transparency of the sector as one of its priority issues. It has funded several relevant projects for quality certification of NGOs since 2005, from the European Social Fund and from the national budget. Two projects worth highlighting were carried out by the CISCC, which developed a Quality Standard for NGOs based the ISO 9001 standard for Quality Management System (QMS) and which developed Minimum recommendations for NGOs on publishing financial data on the internet. Currently, the Office for NGOs is in charge of preparing a new unified law on NPOs, which foresees further measures for enhancing transparency of the sector.

307. Authorities have not demonstrated that the risk-based approach to supervision of NPOs is in place. Different bodies are responsible for oversight of the different legal forms of NPOs and for their different operations and obligations. The Internal Affairs Inspectorate (IAI) of the Ministry of Interior supervises the tasks and activities of associations, requirements related to registration data, and requirements on the associations' assets (prohibition to divide assets among members and obligation to spend surplus income to fulfil the purpose and objectives of the association). Inspection by the IAI only takes place off-site. The MI (responsible for supervising the profitable activities of associations) and FARS (responsible for monitoring implementation of accounting provisions) can also perform on-site inspections.

308. FARS provided statistics on number of on-site inspections of NPOs and number of violations identified. For the period 2014-2016, 307 inspections were carried out. During 127 of the inspections, violations were identified at a total number of 276 violations. Most violations were identified among sports organisations. For humanitarian and charity associations, 13 violations were identified within 3 out of 8 inspections. 91 decisions were issued on payment of taxes issued; 13 decisions were issued in relation to the prohibition of performing activities or prevention of illegal employment. FARS has investigated in 80 cases whether to pursue potential misdemeanour offences; however no criminal complaints against the NPOs were filed.

309. The IAI can impose misdemeanour sanctions on associations at its own initiative or upon request by other bodies. Most sanctions are imposed upon request of the Administrative Units under the Ministry of Interiors (locally responsible for registering associations), the Police, the Market Inspectorate and the Financial Administration. From 2013-2016, the IAI imposed 10 fines and issued 5 warnings, mostly concerning cases in which an association performed an activity that is not stated in its statute.

310. It remained unclear whether other NPOs are supervised with regard to use of funds according to stated purposes; and whether there are any authorities other than the FARS that have the power to conduct inspections, like for associations.

311. According to the OMLP, it has started to deal with the issue of NPOs in 2003/2004. As described in the 4th round MER (p. 118-119), a risk analysis and report were prepared in 2006 regarding the abuse of the non-profit sector for funding terrorism. Although this report was not formally approved by the Government, some of the proposed measures were carried out in subsequent years, in particular legal changes to promote transparency of associations and foundations. From the discussions with the Slovenian authorities at the 4th round on-site it became clear that the 2006 risk analysis was considered a good starting point and would be built upon in future reviews. However, from interviews during the 5th round on-site it did not become apparent that this analysis provided real insight in the FT risks in the sector.

312. Another review of the NPO sector by the OMLP took place in 2012 through a mapping of the sector, review of legal bases for NPOs' establishment and activities and financial analysis of the sector. This review is described in the biannual update report of Slovenia to MONEYVAL in 2015. In general terms, the authorities stressed in this report that due to the relatively large size of the NPO sector, the geo-strategic position of Slovenia and social and cultural connections with higher-risk territories, the possibility exists for FT to be committed in Slovenia. Yet the evaluation team found no evidence that this exercise set out to identify features and types of NPOs likely to be at risk for FT. No final report of the review was published.

313. In the course of the 2015-2016 NRA, the NPO sector was assessed as showing low vulnerabilities for ML/FT abuse due to the fact that NPOs perform their activities mostly in fields related to humanitarian purposes or sports. Yet this assessment seems to be based mainly on the analysis of relevant laws rather than practical experience (for example, cases of suspicions or offences identified) or types of activities or other characteristics of certain organisations that may potentially put them at risk of FT abuse. Thus, the evaluation team concludes that still no in-depth analysis of the sector's vulnerabilities for FT has been carried out.

314. The Action Plan following the 2015-2016 NRA states that systematic and consistent supervision on operations and use of financial funds of NPOs is needed, with a particular focus on organisations that are to a large extent financed on the basis of donations and are not obliged to disclose annual reports. It did not become clear to the evaluation team which proportion of the sector would fall under these criteria. Authorities advised that they estimate that most donations are for NPOs in the area of sports and to associations with a humanitarian status. They further clarified that all NPOs are obliged to submit annual reports to the business registry, but that foundations and religious communities are not under obligation to disclose these to the public.

315. In recent years, there were some cases of suspicion of NPOs being involved in illegitimate activities, which were not confirmed by investigative authorities as being sufficient for further FT investigation. From the information provided during the on-site, the assessment team was assured that LEAs and intelligence services are sufficiently vigilant to the FT risks of NPOs and that they are taking coordinated mitigating actions.

316. NPOs met on-site were in general aware of their obligations and aware of the possible abuse for illicit activities including FT. This level of awareness was not achieved due to governmental outreach activities, but mainly stems from internal rules of NPOs, especially those that are part of international networks, and the need to keep a good reputation.

317. Some outreach activities with regards to NPOs are currently being planned by the OMLP in close cooperation with CISCD, to further increase transparency and to raise awareness of FT risks. The latter organisation was also involved in the process of public consultation on the new APMLFT, which includes measures to further increase transparency in the sector through a register of beneficial owners of legal persons which will include NPOs (see further under IO.5).

Deprivation of TF assets and instrumentalities

318. In practice, no assets have been frozen under UNSCR 1267 or UNSCR 1373 in Slovenia. However, the evaluation team was informed by the authorities of several cases of partial matches detected by financial institutions (banks), which were communicated between the SCG members. In one case, the question was consequently brought to the relevant UNSC Committee. Funds were detained until the issue was resolved, which took approximately two months due to the fact that a response from the UNSC Committee had to be awaited. It was established that this was a case of a false-positive. Banks also confirmed that they have had several cases of potential matches and that they reached out to the authorities (OMLP and MFA) to be certain that they were false positives. The cases were either reported directly to the MFA or first to the OMLP. Authorities advised that, even if there was no exact match, information about the checks undertaken was also disclosed to the police and intelligence. This demonstrates the certain level of effectiveness of the regime regarding the detection of funds possibly related to a listed person(s).

Consistency of measures with overall TF risk profile

319. In light of current developments which have led to increases in the FT risks that the country is exposed to, evaluators are concerned that the current level of the implementation of TFS is not adequate and should be improved. Although authorities have stated that there were no suitable cases so far, the evaluation team is not convinced that sufficient coordination has taken place between authorities to consider whether or not designations at the domestic or international level should be considered. The lack of awareness among many reporting entities on TFS imposed at UN and EU level is a cause for concern in the light of the increased risk profile.

320. Given the relatively large size of the NPO sector, the geo-strategic position of Slovenia and social and cultural connections with higher-risk territories, the evaluation team notes that possibilities exist that FT could be committed in Slovenia through NPOs. Although no special assessment has taken place to identify types of NPOs at risk for abuse, and no risk-based supervision is in place, it appears that authorities do coordinate and implement adequate and serious mitigating measures where potential for abuse has been identified.

Conclusions on Immediate Outcome 10

321. Legal and institutional fundaments for the implementation of TFS in the field of FT are in place in Slovenia, but they suffer from gaps in terms of delays and resources. Coupled with limited awareness of TFS obligations among many reporting entities, guidance which is not fully in line with the standard, and lack of supervision in many sectors, the country's ability to prevent FT flows through the effective use of TFS is weakened.

322. Slovenia has made important efforts to increase transparency of NPOs in order to prevent their abuse for illicit activities, and has good frameworks in place to obtain information on their structures

and oversee their funding sources. However, targeted risk-based measures to assess and mitigate potential FT abuse in the sector are lacking.

323. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 10**

Immediate Outcome 11 (PF financial sanctions)

324. When the comprehensive sanctions against Iran were adopted, Slovenia had a significant bilateral trade with Iran. Authorities were confronted with many questions raised by the private sector and coordinated to provide guidance on implementation of the sanctions. In the case of North Korea (DPRK), Slovenia reportedly does not have any relations, so no specific activities were launched aside from publishing relevant legal acts. Indeed, the evaluation team did not come across evidence of any significant trade or business involvement with DPRK.

Implementation of targeted financial sanctions related to proliferation financing without delay

325. As a member of the EU, Slovenia mainly relies on the EU framework for implementing restrictive measures against DPRK and Iran in line with UNSCRs 1718 and 1737. The practical reliance on the EU framework raises concerns as to whether TFS in the field of PF would be implemented "without delay", should assets of a listed person be detected in Slovenia. Although the Slovene Act on Restrictive Measures (ARM) gives the Slovenian government powers to adopt national regulations transposing UN designations while awaiting EU implementation, these have not been used in practice. The problem of the delay is to some extent alleviated in the case of targeted sanctions relating to proliferation, as compared with FT, because new UN designations are rare and where they occur, it is frequently the case that newly designated individuals and entities by the UN had already previously been listed in the EU framework. With regard to Iran, the EU mechanisms have not suffered from technical problems in the length of time for transposition. Since EU Regulation 267/2012 on Iran was issued in March 2012, there were only two occasions where the UN added designations to the list under UNSCR 1737. In both cases, these individuals and entities had already been listed by the EU. For the DPRK, there have been gaps in transposition on five occasions although these gaps were partly mitigated as 13 out of the 49 additional persons and entities had already been listed by the EU.

326. As explained in more detail in the TC Annex (R.7), national implementing regulations exist in Slovenia on the basis of the Act on Restrictive Measures (ARM) in order to complement the EU framework. These regulations specify fines for breaches of obligations and division of responsibilities for state authorities.

Identification of assets and funds held by designated persons/entities and prohibitions

327. Most financial institutions, banks in particular, confirmed to have integrated sanctions lists in their customer screening and monitoring processes which include PF sanctions regimes. However, there are concerns over timeliness and depth of checks, and certain obstacles in the proper identification of assets and funds held by designated persons/entities regarding checks of the beneficial owner(s) against the sanctions lists, as described under IO.10. There are no mechanisms for identification and detection of assets and funds of designated persons/entities in the DNFBP sector. In practice, no assets have been frozen under UNSCRs 1718 and 1737.

328. According to the authorities and the interviewed banks, there are not many non-residents as banking customers so there are no significant numbers of matches against the sanctions lists. In a case when there is a (partial) match, banks should establish additional information whether customer is the person/entity on the list. Banks have the tools to obtain additional information for its own customers when conducting CDD/EDD. However, if the bank receives a transaction to the customer's account from another/foreign bank, the bank does not have additional information on the sender and it does not conduct additional checks. BoS is preparing guidelines on this topic. In the view of the authorities, the bank should, if such a case occurs, contact the bank where the sender is

customer to obtain additional information in order to establish whether there is a match with the sanctions lists.

FIs and DNFPBs' understanding of and compliance with obligations

329. Financial institutions met on-site demonstrated a certain level of awareness of the existence and the implementation of different sanctions regimes, which would implicitly include those directed to the PF. Generally, they have integrated sanctions lists (including PF) in their IT systems. However, specific awareness of the issue of PF was not demonstrated. The representatives of the DNFBP sector were generally not aware of their obligations under sanction regimes.

330. The MFA has issued Guidelines on the implementation of financial restrictive measures (see IO.10, R.6 and R.7). However, they do not mention explicitly proliferation or proliferation financing sanctions and therefore do not appear well suited to provide adequate guidance on PF. The authorities are convinced that it is clear that the guidelines cover PF, since they cover restrictive measures in the field of terrorism and 'all other restrictive measures which are not related to terrorism and which are associated with third countries including Iran and DPRK . The evaluation team nevertheless believes that explicit mentioning and description of proliferation (financing) sanctions would be highly preferable to promote the public's and private sector's understanding.

331. Authorities met on-site indicated that there are no specific awareness-raising measures regarding PF. The system on informing the public is the same as for other sanctions regimes, with the MFA posting relevant legal acts at its website. A notice was published in the Official Gazette of Slovenia within a day when EU Regulation 267/2012 on Iran was significantly amended in January 2016. However, the authorities do not have a systematic practice of publicizing or proactively communicating changes in listings each time they occur.

Competent authorities ensuring and monitoring compliance

332. The ARM prescribes that supervision of the implementation of international restrictive measures shall be carried out by public authorities as specified in the regulations issued on the basis of the Act and in accordance with the regulations governing their individual supervisory fields. The Iran and DPRNK Decrees issued by the Slovenian Government to facilitate implementation of the EU Regulations specify the applicable misdemeanour sanctions for non-compliance with freezing obligations, and bodies responsible for supervision. However, the Decrees name 'the competent inspection and customs authorities, the police, and the competent holders of public authority' 'within their subject-matter jurisdiction', as responsible for overseeing implementation, which is not very specific. Breaches of international restrictive measures, including for PF, can also be prosecuted as criminal cases (Art. 374a CC), but there has been no such practice.

333. BoS demonstrated certain knowledge on its obligations in monitoring compliance of the banking sector with relevant UNSCRs on the basis of the legal acts mentioned above. As described above, BoS detected certain areas where improvement should be introduced and is preparing guidelines for banks regarding obtaining additional information for the customer in case of possible matches. This shows that BoS is taking certain specific steps towards raising the level of compliance of the banking sector with international sanctions regimes. BoS indicated on-site that supervision of sanctions implementation takes place in the context of AML/CFT supervision. In practice BoS does not conduct specific or targeted on-site examinations relating to restrictive measures. Thus, authorities demonstrated some effectiveness in the supervision of the banking sector, which should be further improved with more specific targeted supervision.

334. Other authorities did not demonstrate adequate supervision of the implementation of UNSCRs relating to the combating of PF. The SMA does not specifically check the implementation of sanctions for the securities sector. The SMA's guidelines include the requirement to respect provisions of the APMLFT, but PF falls outside of the scope of this law. The MI did not consider itself competent to supervise the implementation of TFS. The BoS PSS, supervisor of other financial institutions (eMoney institutions, payment institutions, foreign exchange offices) only establishes whether the supervised

entities have procedures in place to implement sanctions lists, but not the actual implementation. None of the DNFBPs are supervised for implementation of sanctions regimes.

335. The Sanctions Coordination Group (SCG) – the same group as described under IO.10 for TFS in the field of FT – represents a potentially good tool for enhancing domestic cooperation and coordination in the field. There is however still room for improvement of its work. The meetings of the group are not frequent and its work is mainly conducted through written procedures. It appears that not all stakeholders are aware of their important role in the work of the SCG.

336. Members of the group reported on-site that, when sanctions against Iran were still in full force, there have been a few notifications and requests for authorisation of transactions to and from Iranian persons, entities and bodies by Slovenian banks, which were dealt with in coordination by the SCG (by the MFA and Ministry of Finance most notably). Eight authorizations were issued.

337. The members of the SCG can also be consulted by the competent Ministry in the field of dual use goods export control. The Ministry of Economic Development and Technology (MEDT) is generally competent in this field and issues the authorisations or rejections for export of goods to a company that may be on a sanctions list in the field of dual goods. It has its own standing group to support its decision-making process, in which the MFA is also represented. If necessary, the MEDT can also ask for the opinion of members of the SCG that are competent with regards to the business sector that the envisaged export relates to, on the basis of Article 8 ARM. The systems in place demonstrate to a certain extent the coordinated way in which the Slovenian competent authorities approach the issue of counter-proliferation. Authorities met on-site further informed the assessment team on the existence of a case when customs officials, upon cooperation with other relevant authorities, detained goods that were supposed to be exported to Iran. The company was fined and the relevant goods were confiscated. The authorities presented this case to prove their ability to make effective use of the cooperation gateways in place to detect and suppress circumvention of sanctions regimes.

Overall conclusions on Immediate Outcome 11

338. Slovenia has a system in place for the coordination of the implementation of proliferation related sanctions, including PF. Effective use of the system in the context of sanctions against Iran has been demonstrated to some extent.

339. TFS relating to proliferation are in a technical sense not implemented without delay, owing to Slovenia's reliance on the EU transposition of UN designations. However, in the case of Iran, sanctions were implemented without delay as a result of the more extensive EU sanctions regime, and in the case of DPRK the risk posed by delays is largely mitigated by the negligible trade and financial links between Slovenia and DPRK.

340. Most FIs routinely screen customers and transactions against EU and UN TFS lists, but most DNFBPs were not aware of their obligations in the field of PF. No PF-specific guidance has been issued and no awareness-raising activities have been undertaken.

341. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key Findings
1. Banks have a sound understanding of the major sector-specific ML risks, and mitigating measures applied are largely commensurate. The situation varies among non-bank FIs, while DNFBPs lack

awareness of the extent to which they are exposed to ML risks and mostly rely on the banking sector to manage potential abuses.

2. The awareness of FT risks is generally low across all sectors. Banks acting as agents for international MVTS providers demonstrated a relatively higher understanding of FT risks, but lack guidance from competent authorities to apply sufficient risk-mitigating measures. The rest of FIs limit their analysis of FT risks to EU sanctions lists and certain high-risk jurisdictions.

3. Implementation of CDD requirements by FIs improved substantially over the recent years due to increased efforts by supervisors. AML/CFT measures are being tailored to individual conditions of customers. However, the lack of an in-depth and consistent approach to ascertaining beneficial owners and PEPs has an impact on the overall effectiveness of the system.

4. There is a lack of awareness of the activities of the EU passported MVTS provider offering services in Slovenia via an agent, which is running a chain of retail outlets. This raises concerns about the effective application of AML/CFT measures in the remittance business outside of banks.

5. Significant gaps exist in the implementation of CDD requirements in DNFBP sectors. Real estate agents and notaries do not seem to fulfill their gatekeepers' role in facilitating real estate transactions and establishing legal entities. There are also concerns that high risks involved in the business of trading scrap gold are not being adequately mitigated.

6. The OMLP is generally satisfied with the quality of STRs received from banks, but lacks meaningful information from non-bank FIs. The level of reporting among DNFBPs is inadequately low considering their involvement with higher-risk customers and products. FT-related reports are rare and mostly submitted by larger banks.

7. Banks have sound AML/CFT compliance functions that are well-resourced, and involve regular internal audits and trainings. Non-bank FIs have appointed compliance officers, and have basic internal policies and procedures in place, but need specialized training to effectively handle the complexities of AML/CFT requirements. Application of internal controls in DNFBP sectors appears very limited.

Recommended Actions

Slovenia should:

1. Implement the newly adopted APMLFT effectively by developing relevant guidance and applying respective supervisory measures to ensure that obliged entities meet their CDD obligations, particularly with respect to ascertaining beneficial owners and PEPs.

2. Communicate the information and guidance on FT risks to obliged entities, and ensure that adequate risk-mitigating measures are reflected in their internal policies and procedures.

3. Enhance cooperation with home country supervisors concerning the MVTS provider and other FIs operating in Slovenia under the EU passporting regime to make sure that they are sufficiently aware of ML/FT risks and effectively apply AML/CFT measures.

4. Ensure that DNFBPs are adequately aware of ML/FT risks, report suspicious transactions and implement other AML/CFT requirements.

5. Consider allowing obliged entities to verify the validity of identity documents of natural persons in relevant public databases.

342. The relevant Immediate Outcome considered and assessed in this chapter is IO.4. The recommendations relevant for the assessment of effectiveness under this section are R.9-23.

Immediate Outcome 4 (Preventive Measures)

Understanding of ML/FT risks and AML/CFT obligations, and Application of Risk-Mitigating Measures

Financial Institutions

343. The banking sector accounts for the prevailing majority of the financial services industry in Slovenia and is most vulnerable to ML/FT threats. There were 13 banks[59] operating in Slovenia by the time of the on-site visit: seven domestic and six foreign banks. The latter are subsidiaries of EU-based parent banks, while only one domestic bank has subsidiaries abroad (Balkans). The level of financial inclusion is high with 97% of the population maintaining bank accounts, and cash payments for goods and services exceeding EUR 5,000 prohibited. Banks' customers are predominantly natural persons (over 90%). The share of non-residents in the overall customer base is estimated at 2.2% among natural persons and 0.8% among legal entities.

344. Banks demonstrated a proactive assessment and consideration of major sectoral ML risks. The supervisory activities carried out by the BoS have apparently increased the banks' awareness of their role as gatekeepers, and facilitated the development of elaborate systems for profiling and managing ML risks. However, the understanding of FT-related risks is relatively low. Most of the banks limit their analysis of FT risks to the EU sanctions lists and certain higher-risk jurisdictions, while some larger banks acting as agents for international MVTS providers do also consider wire transfers and inability to adequately identify asylum-seekers from the recent migration crisis as major vulnerabilities. All banks interviewed expressed the need for more guidance and training on the identification and effective handling of FT risks.

345. Banks perceive as their main challenge the cross-border transfer of funds, particularly from offshore jurisdictions and neighbouring countries with serious tax evasion problems and organized criminal activity, and subsequent cash transactions involving (foreign) straw men. Attempts to invest illegal proceeds in real estate purchases by non-resident customers that frequently involve setting up of legal entities and fictitious business arrangements were also highlighted as a serious concern, which matches with the conclusions of the NRAs. The BoS's inspections in 2012-2013 resulted in the creation of special committees inside banks to review existing customer portfolios and introduce better risk-management processes. This led to the termination of business relationships with multiple legal entities from offshore jurisdictions and the application of enhanced CDD measures in relation to remaining higher-risk customers. Banks also introduced stricter client acceptance policies and upgraded IT-based transaction monitoring systems. Further risk-mitigating measures included training of customer-facing staff to better understand the purpose and intended nature of business relationships, and setting up of lower caps and prior notification requirements on cash withdrawals.

346. Banks classify business relationships based on a number of risk factors (e.g. geography, client type and activities, nature of products). The high-risk identifiers used by banks are mainly based on supervisory guidelines and group policies, but relevant risk models and indicators are also generated internally. Higher-risk customers are less than 3% of banks' clientele and include non-residents (e.g. Balkans, Italy and Russia) and customers from higher-risk jurisdictions, as well as offshore corporate structures and certain types of businesses (e.g. virtual currency exchange platforms). Banks apply differentiated CDD measures based on the attributed risk by obtaining additional data on the source of funds and activities of customers, and conducting more intense scrutiny of their transactions.

347. The insurance sector is the second largest in the financial services industry; however ML/FT risks are considered low given the nature of insurance business in Slovenia. The domestic life insurance market is smaller compared to most of the EU countries, while the amount of cash transactions is negligible and the number of non-resident customers insignificant. Nonetheless, interviews demonstrated that effective measures are being implemented to manage inherent vulnerabilities of insurance products involving investment elements. Insurance companies mostly classify their customers based on risk factors set out in the APMLFT and supervisory guidelines. Less than 1% of customers are regarded as higher-risk and are subject to relatively intensive on-going monitoring measures. Evaluators were also informed that surrender clauses in life insurance policies

[59] The number of banks decreased to 12 due to an acquisition process that was finalized in January 2017.

are quite restrictive and third party payment of premiums is not allowed unless a reasonable connection is ascertained between the payer and the policy-holder or the beneficiary. Changes of beneficiaries in life insurance policies that lack reasonable rationale are treated as higher-risk situations and thus, enhanced CDD measures are applied, which may also include the identification of beneficial owners of beneficiaries.

348. Slovenia's capital market is very small and has been severely hit by the recent financial crisis. Securities business is conducted by banks and other investment service providers (brokerage firms and asset management companies). Although the latter classify customers based on risk, their AML/CFT expertise is less well developed compared to banks. Some of the investment service providers met on-site claimed that no business would be done with customers when risks are considered too high. Others had difficulties in explaining specific measures that would be taken in higher-risk situations. Overall, the securities sector sees itself as low risk since cash is only accepted into custody through a special bank account and the number of transactions is relatively low, which allows for their closer scrutiny.

349. The majority of MVTS are concentrated in the banking sector. There are four banks acting as agents for two international MVTS providers and offering international money transfers. The understanding of ML/FT risks in the sector is relatively high, and controls applied include lower caps on transfers to higher-risk jurisdictions and certain FT scenarios built in transaction monitoring systems. However, the banks met on-site admitted to having difficulties in understanding intentions of occasional customers, including asylum-seekers, carrying out cross-border wire transfers and expressed the need for more guidance to effectively manage FT risks. Moreover, one of the international MVTS providers has recently started providing its services in Slovenia under the EU passporting regime and using an agent, which is running a chain of retail outlets (convenience stores) spread across the country. The domestic authorities met lacked awareness of their activity, nor did they have precise plans on how to make sure that higher risks involved in the remittance business outside of banks are appropriately mitigated.

350. There are 22 leasing companies and 68 credit institutions registered in Slovenia that provide consumer loans averaging EUR 20,000 for cars and EUR 5,000 for other goods. The sector considers itself low-risk, since cross-border activities are not performed and the number of foreign customers is very small. Interviews demonstrated that customers are classified by certain risk factors and those regarded as higher-risk are required to provide information on the source of funds. There are however more than 300 credit institutions operating in Slovenia through the EU passporting regime. The domestic authorities do not have any information about their activities, which raises concerns about the adequacy of AML/CFT controls applied in the sector.

DNFBPs

351. The understanding of ML/FT risks is generally less well developed among DNFBPs compared to the financial sector. Although all obliged entities are required to analyse ML/FT risks in their activity and act accordingly, DNFBPs rarely apply the risk-based approach to business relationships. Some of the DNFBPs met on-site stressed that they usually rely on banks to mitigate ML/FT risks.

352. Real estate agents provide the full service brokerage to their customers, which includes finding potential buyers, providing legal assistance (e.g. drafting contracts), and assisting in the relationship with tax authorities and notaries. Custodial deposits are also accepted to facilitate financial transactions between the parties. Although the real estate sector was identified as one of the most vulnerable by the NRAs, real estate agents met on-site contested the assertion. They claimed that customers seeking to invest proceeds of crime in real estate would not use their services, since it is not obligatory. Thus, real estate agents are aware of some basic CDD requirements, but do not tailor specific measures based on risk. They consider that any inherent threats are being mitigated by banks effectuating payments, however there are also indications that cash payments for real estate do occur. The MIRS, which acts as the supervisory authority for real estate agents, stated that higher ML risks were present in the construction sector, which was not explored in the NRAs.

353. Notaries' awareness of threats inherent to their role in the economic system is quite low. Their involvement in the company formation has been somewhat limited since the government started providing one-stop company and business registration services (one-stop shops). However, setting up of relatively complex companies, including those identified as posing risks of abuse by authorities met on-site (e.g. having share capital contributed in kind), and certifying transfers of shares are still part of notaries' primary duties (see IO.5). Moreover, for a real estate transfer to take place, notaries' must verify signatures of parties to the contract. Although not legally required, when notarial deed is drafted at the request of parties, notarial escrows are sometimes used to facilitate real estate transactions. There are concerns that notaries apply quite limited CDD measures as part of their highly standardized business process without having regard to the actual risks.

354. Only two registered dealers of precious metal and stones exist in Slovenia, although there are many other scrap gold traders operating on the market extensively. Domestic authorities lack information about the number of the latter or the nature of their activities. OMLP detected the increased activity of scrap gold traders from one EU country a few years ago. The cross-border element of the business was confirmed by other interlocutors during the on-site visit. The registered dealer met claimed that it exclusively trades investment gold, and appeared to be aware of major sectoral risks and some basic AML/CFT requirements. However, neither registered dealers nor scrap gold traders are subject to any AML/CFT supervision. There are also concerns in relation to the existing practice of trading gold through virtual currency exchange platforms as dealers appear to rely on these platforms to apply CDD measures and on domestic banks to address inherent vulnerabilities.

355. There are 10 land based casinos in Slovenia that are mainly located near the border with Italy trying to attract Italian nationals. The latter make up the majority of their high-value customers and also frequently feature in the major ML typologies in the banking sector. Casinos' awareness of risks is limited to unfamiliar customers, large amounts of cash, and collusion between players and employees. Although winning certificates are rarely issued, cash deposits held by casinos as well as certain winnings could be exchanged to bank cheques at the request of customers. The mitigating measures are focused on the identification of players at the entry. Cash payments are registered at the cashier's desk, but not at gaming tables, which provides the possibility for the cash being circulated without the knowledge of a cashier. Casinos also follow the behaviour of players through video surveillance, but mainly to enforce "fair play" rules. There is only one e-casino registered in Slovenia, which is subject to strict controls by the supervisor. The e-casino is aware of major sector-specific risks and applies mitigating measures such as prohibiting multiple accounts, preventing payments to third parties and identifying collusions.

356. Lawyers have very limited awareness of risks and consider AML/CFT obligations as an excessive burden due to the nature of their activities. The number of lawyers per capita in Slovenia (more than 1,000 sole practitioners and around 250 law firms) is below EU average and thus the market does not appear squeezed, although it is unclear how many of them actually perform services falling under the scope of the APMLFT. The law firms met by evaluators confirmed that they do not classify customers by risk and take comfort in CDD measures applied by banks. Both the firms and the Bar Association contested the NRAs' assertion that lawyers frequently use cash in their dealings with customers by withdrawing funds transferred to fiduciary accounts and handing them over in cash. They also claimed that customers' funds are not typically managed by lawyers, while fiduciary accounts (mostly pooled bank accounts) are merely used to receive and disburse damages awarded by courts. It appears that banks do identify beneficiaries of such fiduciary accounts. The practice of setting up and selling so called "shelf companies" by lawyers also highlighted in the NRAs does not seem to persist due to recently introduced restrictions on the establishment of legal entities (see IO.5).

357. Auditors, accountants and tax advisors lack awareness of ML/FT risks even though their customers include legal entities from offshore jurisdictions. Audit firms also appear to perform such services as the management of customers' funds or setting up of companies. Tax evasion was

identified as a potential problem, but those interviewed by evaluators did not think it was connected to the ML offence. Accounting and tax advisory services are performed by a large number of entities (more than 4,000) and most of them are small companies or self-employed sole entrepreneurs, which complicates the availability of resources for AML/CFT purposes. However, the audit market is much less fragmented. There is also no meaningful AML/CFT supervision performed in any of these sectors, although auditors do have an oversight body with adequate supervisory powers and the new APMLFT gives OMLP the extended mandate to supervise accountants and tax advisors.

Application of CDD and Record-Keeping Measures

Financial Institutions

358. FIs demonstrated a generally high awareness of CDD requirements. Institutions met on-site claimed that the implementation of AML/CFT measures improved substantially over recent years largely due to intensified supervisory efforts. Evaluators were also informed that the number of violations identified by supervisory bodies during inspections declined significantly since 2013. Nonetheless, systematic breaches were uncovered in a relatively smaller bank in 2015, although the BoS indicated that the bank's awareness of the importance of AML/CFT compliance improved with the arrival of new ownership and the application of relevant supervisory measures.

359. Due to data-protection concerns, FIs are not allowed to have access to the Identity Card Registry, which is considered as one of the sectoral vulnerabilities by the NRAs. Moreover, FIs were until very recently prohibited from maintaining electronic copies of identity documents of natural persons, although the new APMLFT provides for such a possibility. This has apparently partially limited the ability of FIs to check the validity of identity documents as part of the customer verification procedure. However, banks met on-site claimed that they provide relevant trainings to their employees and use external web-applications (e.g. EU Public Register of Authentic Travel and Identity Documents) that helped them uncover instances of identity fraud on a number of occasions.

360. FIs were recently given the possibility to search in the Business Register whether an individual is a founder, partner, representative or member of the supervisory board in domestically-registered legal entities. This has substantially improved FIs' ability to verify the business activities of natural persons. However, evaluators have some concerns regarding the reliability of the data kept in official registries of different types of legal entities that are interconnected with the Business Register (see IO.5).

361. There are concerns about the depth and consistency of the verification of beneficial owners. FIs mostly use official registries of legal persons that do not require disclosure of their entire ownership structure, and seek additional data from customers. Banks also check foreign databases and receive support from parent groups. However, the on-site interviews revealed certain gaps in the understanding of the concept of beneficial ownership. In particular, the difference between beneficial ownership and ownership interest is not fully appreciated, and thus, natural persons holding relevant management positions or exercising indirect control over the customer are not always sought after. This is particularly true of those non-bank FIs that have less sophisticated AML/CFT expertise.

362. There also appears to be a degree of over-reliance on customers' written statements when the data on beneficial owners is not conclusive. A number of FIs met on-site, mostly banks, were convincing in their claims that business would not be done unless the ultimate natural persons behind the customer were ascertained based on independent information sources. However, the rest acknowledged that they would rely on the customer's declaration when the ownership structure turns complicated. It was indicated that an entirely Slovenian-incorporated company posed no difficulties in this regard, while involvement of foreign legal entities in the chain of ownership could render the verification of beneficial owners extremely challenging. The evaluators were not given statistics on the number of legal entities with such relatively complex structures involving foreign ownership element to form a more complete view on the subject.

363. The awareness of the characteristics of trusts and other legal arrangements is quite low as they cannot be formed under the domestic legal framework (except for mutual investment funds) and are rarely encountered by FIs. Only banks reported having trusts as part of the ownership structure of their customers, although in very small numbers. Banks also admitted to facing difficulties in identifying beneficial owners of trusts, and expressed the need for more guidance from supervisors on how to deal with unfamiliar legal structures in general. The new APMLFT introduced more detailed requirements on the identification of trustees, settlors and beneficiaries of trusts, and this may help clarify the obligations of FIs.

364. Ongoing monitoring mechanisms vary across the financial sector. Banks engage in daily transaction monitoring with the help of sophisticated IT systems that employ built-in scenarios to identify unusual activities or connections, while non-bank FIs typically examine transactions on a weekly or monthly basis. Checks are generally tailored to the risk level. Banks apply a more elaborate risk-based approach by conducting extensive checks on higher-risk customers. Insurance companies and investment service providers other than banks follow provisions of the APMLFT and supervisory guidelines, which typically implies obtaining more information on the sources of funds and frequent updates of customer data.

365. Reliance on third parties is permitted by the APMLFT, but rarely practiced and banks are mostly relied upon for this purpose. The general understanding among FIs is that the assessment of the quality of AML/CFT controls is not needed in relation to EU-based banks, as well as their branches and subsidiaries in third countries. Some of the banks apply stricter group-wide policies and would only rely on members of the same group to verify authorized representatives of customers, but not their beneficial owners.

366. FIs are well aware of their record-keeping obligations, and maintaining customer identification data, account files and business correspondence is the norm. The supervisory authorities have not identified any serious deficiencies in this respect.

DNFBPs

367. Application of CDD and record-keeping measures varies among DNFBPs, but is generally much less comprehensive compared to the financial sector. The relevant supervisory guidelines exist, however DNFBPs are not subject to meaningful AML/CFT supervision to ensure adequate level of compliance. While identification of customers is the norm, information on their beneficial owners is rarely obtained and the concept of the risk-based approach is unfamiliar.

368. Real estate agents and notaries obtain only basic identification data and the tax number of customers, however the former identify only buyers and not sellers of the property. Although reference was made during the on-site visit to checks conducted in the Business Register, there is a limited awareness of beneficial ownership requirements. Real estate agents and notaries also do not seem to examine the sources of funds involved in real estate transactions, but rely on banks to carry out full CDD measures when effectuating payments.

369. The registered dealer in precious metals and stones met on-site appears to identify customers, but not their beneficial owners. Customers are not identified when the trade occurs via a virtual currency exchange platform, which is presumed to apply adequate AML/CFT measures as an EU-based registered payment institution. Overall, the sector appears to be extremely fragmented and authorities lack information on the state of application of CDD and record-keeping measures by both registered dealers and numerous scrap gold traders.

370. Land based casinos have some basic CDD measures in place that focus on the identification of customers upon entry, and subsequent monitoring mostly to prevent collusion between players and enforce “fair play” rules. The only e-casino registered in Slovenia applies special software to monitor transactions of its customers. Overall, casinos do not appear to request provision of information on the source of funds.

371. Lawyers met on-site indicated that they apply basic CDD measures to the extent required for conducting their business. This usually consists of identifying customers and verifying the authority of their representatives. However, the ownership chain of legal entities is not examined to ascertain ultimate beneficial owners. The Bar Association lacks information on the level of compliance with CDD and record-keeping requirements within the legal profession.

372. Auditors have some basic know your customer policies in place, whilst accountants and tax advisors met on-site had a very general idea of CDD requirements and only referred to certain background checks on customers carried out at the beginning of business relationship. Auditors identify beneficial owners of legal entities by examining internal documents and obtaining customer declarations. Their understanding of beneficial ownership is however limited to shareholders and authorized representatives.

Application of Enhanced or Specific Measures

PEPs

373. The requirements of the APMLFT have until very recently applied exclusively to foreign PEPs. Thus, only one bank claimed during the on-site visit that it has also been identifying domestic PEPs as part of group-wide policy. The issue of domestic PEPs is of importance in the Slovenian context due to concerns about corruption (see IO.1).

374. The majority of banks met by evaluators demonstrated that they have put in place appropriate risk-management systems to determine whether customers are foreign PEPs. This includes checking external (commercial) databases on PEPs during the customer on-boarding process, as well as undertaking periodic checks on existing relationships to ascertain changes in status, although the difficulty of identifying close associates was stressed. The rest of banks and other FIs rely on written declarations obtained from foreign customers and sometimes conduct internet searches to clarify their status.[60] Among DNFBPs, only casinos showed a degree of awareness of the requirements related to foreign PEPs, but admitted to having difficulties due to the lack of access to relevant databases.

375. FIs treat all foreign PEPs as higher-risk customers, but the application of specific measures varies across sectors. Insurance companies indicated that approval to establish a business relationship with PEPs is given at the level of board of directors, while branch managers and heads of compliance departments are the relevant decision-makers in most of the banks. FIs usually request a statement on the source of funds from foreign PEPs, but not on the source of wealth and obtain additional data on their activities. All of the FIs met on-site reported that they find confusing the requirement to obtain information about the "source of property" of PEPs introduced by the new APMLFT. This indicates the need for a closer engagement of competent authorities with obliged entities on the implementation of provisions of the new law.

Correspondent Banking

376. Awareness of requirements related to the establishment of correspondent banking relationships is generally high. However, the assessment of the quality of AML/CFT controls and the application of other required measures take place mostly in relation to non-EU based respondent institutions. Only one bank among those met on-site claimed to apply checks on the quality and reputation of EU-based institutions as part of group-wide policy. The questionnaires and Swift KYC register of correspondent banks are used to obtain the information on potential respondents. Banks also make sure that correspondent relationships do not involve shell banks, while payable-through LORO accounts are not allowed.

New Technologies

[60] The BS sent a circular letter to banks in February 2017 to make clear that all of them are expected to use external (commercial) databases on PEPs in order to fulfill the requirements of the new APMLFT.

377. Banks offer relatively sophisticated products to customers and those met on-site confirmed that AML/CFT compliance teams are always consulted before the introduction of new products and services. Internet and telephone banking are treated as higher-risk and potential users are required to meet bank officials face-to-face. One of the banks mentioned the example of pre-paid cards that are yet to be introduced but will be dealt with as a higher-risk product.

Wire Transfers

378. There are gaps in the existing legal framework since the inclusion of beneficiary information in wire transfers is not required. However, banks met on-site claimed that messaging systems would block transfers unless all required beneficiary data (name and account or unique reference number) is provided. Data-integrity checks are also carried out to make sure that valid information is included in payment instructions.

379. Banks consider that wire transfers involve higher ML/FT risks, and always ask about the sources of funds and purpose of transactions. Banks appear to verify beneficiaries of transfers when acting as recipient institutions and also pay attention to the beneficiary when considering the risks related to a particular transaction. Existing wire transfer systems ensure that both senders and beneficiaries are screened against UNSCR sanctions lists.

Targeted Financial Sanctions Related to TF

380. FIs met on-site demonstrated a basic level of awareness of FT-related targeted financial sanctions (TFS). However, their implementation is hindered by delays in the transposition of UNSCR lists into the EU legislation (see IO.10). This deficiency is partially remedied in practice as most of the banks and some other non-bank FIs use software systems that directly integrate updated UNSCR lists and check every new customer and transaction against them. However, checks on existing customers in some FIs are only applied periodically. These measures also do not always cover beneficial owners of legal entities and almost no attempt is made to identify funds that are indirectly controlled by UN designated persons. Only one bank claimed that it has been using a group-wide list of entities linked to UN designated persons.

381. FIs seem to understand their obligations once individuals or entities subject to TFS are identified. Examples were provided of funds being blocked and competent authorities alerted when potential matches were identified. However, FIs also expressed the need for quicker responses from competent authorities when FT-related submissions are made. DNFBPs interviewed were generally unaware of the existence of TFS.

Higher-Risk Countries Identified by the FATF

382. The general awareness of the FATF list of higher-risk countries is high among FIs. The FATF public statements are published on the website of OMLP. Although there has been no legal requirement to apply enhanced CDD measures with respect to customers from these jurisdictions until the adoption of the new APMLFT, some elements of enhanced CDD, such as requesting the source of funds, are usually applied in practice. Senior management approval is also obtained in relation to customers from some of the countries on the list (e.g. Myanmar and Syria), while business is typically denied to customers from Iran. DNFBPs met on-site were generally unaware of the existence of higher-risk countries identified by the FATF.

Reporting Obligation & Tipping off

383. The number of STRs has been steadily increasing over the recent years (from 178 in 2010 to 464 in 2015), yet the vast majority of reports are submitted by banks (more than 90% in 2015). The overall increase in the number of STRs seems to be the result of improved appreciation of the importance of ML/FT risk management by banks, which translated into elaborate IT-based transaction monitoring systems and much better resourced AML/CFT compliance functions. The BoS has been monitoring potential defensive reporting practices and applied supervisory measures when it concluded that STRs submitted by a bank aimed at formally meeting its obligations without

adequately examining unusual transactions. Attempted suspicious transactions are also being reported by banks, although their proportion in the overall number of STRs could not be ascertained. In general, the banks met on-site demonstrated a good understanding of reporting requirements and appeared knowledgeable when discussing relevant typologies.

384. The level of reporting beyond banks is quite low, which is inconsistent with high ML/FT risks identified in some of the sectors. For instance, investment of proceeds of crime in real estate and abuse of legal entities are considered as common forms of ML in Slovenia; however very few STRs are generated from real estate agents and notaries. The picture of STR filling is similar when it comes to casinos that extensively deal with higher-risk customers, and auditing/accounting firms and tax advisors even though tax evasion is the most frequent ML predicate offence. The only relatively upward trend in reporting is observed among registered dealers of precious metals and stones.

385. The inadequate level of reporting among DNFBPs seems to be the consequence of limited awareness of reporting requirements. Most of the DNFBP representatives met on-site claimed that suspicious customers would rather be turned down than reported to OMLP. Some thought that only suspicions of ML and not those of funds being proceeds of criminal activity are subject to reporting. Thus, auditors and accountants explained that potential tax evasion cases would perhaps not be reported as they do not constitute ML. Significant gaps in the CDD process and overreliance on banks to mitigate risks are also to blame for a very low number of STRs.

386. OMLP expressed satisfaction with the general quality of STRs received. It was indicated that the absolute majority of reports submitted by the banking sector (up to 80%) includes all relevant data and sufficient justification, but there is still room for improvement, especially when it comes to the provision of information on suspected predicate offences. The statistical data related to the usage of STRs by OMLP and LEAs paints a slightly mixed picture about their actual quality and usefulness. Only about one third of STRs are proved to be unfounded by OMLP, while the rest are disseminated to LEAs and tax authorities. However, the number of disclosures subsequently triggering criminal investigations and prosecutions is much lower. On the other hand, this data must be treated with caution as high evidentiary standards seem to be the major reason for such a discrepancy, rather than the quality of STRs (see IO.6).

387. Obliged entities are informed by OMLP when the suspicion in an STR is confirmed. More in-depth feedback on the quality of STRs is provided through trainings and workshops. Annual meetings are held with AML/CFT compliance officers of banks to discuss STR fillings, and new trends and typologies. However, training seminars have rarely been organized for DNFBPs in the last several years, which reflects the need for a closer engagement with DNFBP sectors on ML/FT prevention issues.

388. OMLP and other supervisory bodies developed red-flag indicators for each type of obliged entities to assist them in identifying suspicious transactions, but the indicators have not been updated since 2010. Some of the non-bank FIs met on-site stated that they exclusively rely on these pre-defined indicators, although they are not supposed to be exhaustive, and do not develop their own. Given the low number of STRs from these sectors, OMLP may be missing important information on some of the suspicious transactions and activities that could be occurring in practice. Several instances of non-reporting by banks have also been identified by OMLP and BoS, but were directly raised with banks without commencing formal proceedings and applying sanctions.

389. FT-related reports have only been submitted by larger banks. Banks have put certain FT scenarios in their IT-based transaction monitoring systems. Potential FT cases described on-site included customers buying plane tickets to destinations en route to conflict zones. However, the rest of FIs met on-site limit their analysis to checking EU sanctions lists and transactions involving certain higher-risk jurisdictions. All of them expressed the need for more guidance to identify and report FT-related activity or transactions.

390. No issues were identified with the tipping-off prohibition during the on-site visit. The existing legal framework however does not allow obliged entities to refrain from the application of CDD

measures when this might alert the potential perpetrator. FIs were familiar with the legal requirement in relation to tipping off, but do not seem to have elaborate procedure on how to prevent disclosure and stated that senior management would be consulted if parties to a suspicious transaction start asking questions.

Internal Controls and Legal/Regulatory Requirements Impeding Implementation

391. Increased supervisory actions by the BoS in recent years resulted in the appointment of competent compliance officers and appropriate positioning of the AML/CFT function inside banks. The number of deficiencies identified during inspections by the BoS, including those related to internal AML/CFT systems and controls, dropped markedly. However, systematic breaches were recently uncovered in a relatively smaller bank which involved repeated disregard of reports of the AML/CFT compliance officer by senior management. Although relevant proceedings were initiated by the BoS against the bank, no fines were subsequently imposed as the process proved lengthy. The protracted nature of proceedings seems to be a persistent problem that impedes the ability of the BoS to impose pecuniary sanctions (see IO.3).

392. All banks have AML/CFT compliance teams that are typically part of larger compliance departments, but some of them appear to directly report to the board of directors. No shortage of dedicated AML/CFT employees was identified. AML/CFT compliance officers met on-site were quite knowledgeable when discussing AML/CFT issues and indicated that they are usually consulted in higher-risk situations, although no such legal requirement exists. They also appear independent in deciding whether to file an STR. Banks routinely screen their staff members for professional qualifications and criminal records, but higher standards apply to AML/CFT compliance officers. The latter are subject to fit & proper checks designed for the senior executive level in some larger banks, where the AML/CFT compliance function is defined as a key function.

393. Banks implement annual training programs for employees, which include introductory trainings for the newly recruited staff. Employees also receive updates about new developments in the AML/CFT field. The Banking Association was credited for organizing frequent training seminars that involve representatives from the BoS and OMLP. Internal AML/CFT systems in all banks are subject to regular independent audits, which appear effective. One of the banks indicated that its internal audit procedure helped identify problems with communication between different organizational units that resulted in the failure to identify beneficiaries of custodial accounts administered by a foreign asset management company and difficulties in checking EU sanctions lists. Necessary arrangements were since made to improve internal communication processes.

394. Only one Slovenian bank has subsidiaries abroad. It claimed that the enforcement of group-wide internal controls is monitored through questionnaires and on-site visits, which sometimes result in the issuance of specific recommendations. Annual meetings involving all subsidiaries take place to discuss relevant AML/CFT issues and related challenges. The BoS also conducted on-site supervision of one of the subsidiaries in Bosnia and Herzegovina jointly with the host country supervisor to check the effectiveness of internal controls and policies. There are no legal or regulatory requirements that would hinder the sharing of CDD information between group members. A number of banks met on-site confirmed that such an exchange takes place.

395. The quality of AML/CFT internal controls outside the banking sector generally falls short of the required standard. While some non-bank FIs have quite well-organized and professional AML/CFT compliance functions, others would benefit from specialized training in the implementation of AML/CFT requirements. The situation varies among DNFBP sectors depending on the size and resources available. Most of them have compliance officers and deputies that typically also have major responsibilities other than those related to AML/CFT issues. Only casinos and the registered dealer of precious metals and stones met on-site demonstrated existence of some basic internal control infrastructure.

Overall Conclusions on Immediate Outcome 4

396. In reaching the conclusion on the overall rating of IO.4, the evaluation team considered that banks showed a sound understanding of major sectoral ML risks during the on-site visit, and clear progress in the application of AML/CFT measures was evident from the interviews with both AML/CFT compliance officers and competent authorities. However, evaluators observed a relatively low level of awareness of banks when it comes to FT risks. While progress in the implementation of CDD requirements by non-bank FIs was also recognized, the lack of awareness about the activity of the EU passported MVTS provider using an agent outside of banking sector was deemed as a reason for concern. Gaps in the understanding and mitigation of risks by real estate agents and notaries also negatively affected the rating since the investment of proceeds of crime in real estate and abuse of legal entities were named as common forms of ML during the on-site visit.

397. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

1. Supervisors are effective in preventing convicted criminals of having control or management positions of obliged entities. However, there is concern regarding supervisors' ability to detect and prevent people with a criminal background and their associates gaining ownership or management positions in these institutions. With regard to DNFBPs and FIs (other than banks, payment and e-money institutions, insurance and securities companies), there is no ongoing mechanism to check the fit and proper status of those individuals that have already been authorized.

2. Despite money or value transfer service (MVTS) providers being identified in the NRA as highest risk, one agent outside of banks has been operating under EU passporting rules through multiple outlets without the knowledge of the authorities. This raises concerns about the provision of adequate control of ML/FT risks in these institutions.

3. Whilst the NRAs have improved the understanding of the supervisors involved in the process regarding the risks in their sectors, there is no ongoing mechanism for cooperation amongst supervisors and with the OMLP in better understanding the risks on a national and sectorial level. The department of BoS responsible for banking supervision has a good understanding of the sector risk of ML and specific risks of the banks under its supervision. Other supervisors have a lower level of understanding.

4. All supervisors have limited understanding and knowledge regarding specific FT issues in their area of responsibility.

5. The BoS has adopted a risk-based approach to ML/FT supervision which takes relevant ML/FT parameters into account. Other supervisors have no risk based approach to supervision for ML/FT issues and the OMLP has not yet developed a strategy for using their newly acquired supervisory powers.

6. The supervisors in the banking, insurance and securities sectors have demonstrated that their actions have had a positive effect on compliance by entities under their supervision, however this has not been demonstrated by other supervisors.

7. Supervisors very rarely impose severe sanctions even in cases of recurrent or systematic breaches, which raises doubts about their ability to deter serious recurring noncompliance by obliged entities.

8. There are genuine efforts being made by representative associations in collaboration with the OMLP and competent supervisors to educate the obliged entities regarding their AML/CFT obligations. However these have been effective only in the banking, insurance and securities sectors.

Recommended Actions

Slovenia should:

1. Continue implementing the risk-based approach of supervision in the banking sector and improve the effectiveness of inspections in all other sectors by implementing a risk-based approach and targeted or thematic inspections when relevant. In this regard the OMLP should urgently implement its supervisory powers and ensure it has the necessary resources.

2. Take steps to improve the knowledge of supervisors regarding ML/FT risks with specific emphasis on FT risk whilst improving the sharing of information between supervisors and the OMLP.

3. Implement additional measures to allow supervisors to check the criminal background and connections of individuals exercising control and management or supervisory board members of obliged entities, including obtaining information from other LEAs and tax authorities..

4. Identify properly the risks arising from the operation of FIs that operate in Slovenia under EU passporting rules, take supervisory actions to mitigate ML/FT risks and enhance the cooperation with the relevant home supervisors.

5. Consider, where appropriate, the use of more severe sanctions, including financial sanctions, in cases of serious recurring noncompliance by obliged entities.

398. The relevant Immediate Outcome considered and assessed in this chapter is IO3. The recommendations relevant for the assessment of effectiveness under this section are R26-28 & R.34 & 35.

Immediate Outcome 3 (Supervision)

Licensing, registration and controls preventing criminals and associates from entering the market

Banks

399. The BoS requires anyone applying for a bank license to provide information regarding individuals exercising control specifically referring to beneficial owners as well. Information is collected using a detailed questionnaire that includes questions about criminal and regulatory background of the applicant and places where he had ownership or management positions. The questionnaire includes questions about various matters that have an implication on prudential and reputational matters and refers to events both in Slovenia and abroad. The information collected also includes information on the source of funds. Similar questionnaires must also be filled out by management and supervisory board members. In addition to checking applicants' conviction records, the BoS, regularly require information from other supervisors in Slovenia and abroad and conducts its own internet search for publically available information. The BoS receives information on convictions but does not have access to information on applicants, held by LEAs or the tax authorities. The application procedures do not include elements that specifically target associates of individuals exercising control and management or supervisory board members.

400. The BoS has used its powers to refuse authorisation of board members based on prudential issues but there have been no grounds for such actions on the grounds of not meeting the 'good standing' requirements. In the case of a recent acquisition of a controlling interest in a bank that was previously government-owned, the BoS conducted extensive checks in collaboration with the European Central Bank (ECB). Although there are no regular ongoing background checks conducted regarding board members, when a particular issue arises it is assessed by the BoS. For example, BoS considered revoking the license of a board member of a bank who was deemed responsible for AML/CFT breaches found in an on-site inspection, on the grounds of prudential issues.

401. In addition to the procedures described above, every bank is required to conduct its own fit and proper tests for board members and employees that hold a key function. The banks' procedures in this regard are subject to BoS supervision.

Securities sector

402. Qualified holders of broker companies and asset management companies (above 10% holding not including beneficial owners and the senior managers of these firms are required to fill in a questionnaire which includes questions on criminal matters by SMA. The SMA checks court conviction records and conduct their own internet searches. In case of qualified holders only they also seek the OMLP's opinion. These procedures do not include elements that specifically target associates of individuals exercising control and senior managers. Portfolio managers are not licensed.

403. On an ongoing basis every SMA inspection also examines the current 'fit and proper' status of the above persons. In addition to this, the firms are obliged to provide information regarding anything that can have a major impact on the company and this includes for example a criminal investigation of a director. It is not clear to what extent this requirement is enforced.

Insurance

404. As regards insurance companies, natural persons controlling the firm, directly or indirectly , and members of the supervisory or management board are required to fill in a questionnaire and show that they have good repute and no final criminal convictions. The ISA relies on information provided by the company and in cases where internet searches conducted by them raise doubts they contact the competent authority or the person involved and seek further information. These procedures do not include elements that specifically target associates of individuals exercising control and management or supervisory board members.

405. The ISA has demonstrated that efforts are made to uncover information about shareholders in an insurance company, including a request for information from a foreign supervisor. However, the limitations placed on the use of information provided do not enable Slovenia to stop criminal elements from controlling an important institution.

Other financial institutions

406. The licensing process for e-money institutions including payment institutions is also conducted by the BoS (different department to banking supervision). There is a list of documents that must be provided, all natural persons in the chain of control are checked for criminal convictions and an internet search is conducted. Since there are very few applications for a license additional checks are decided on a case-by-case basis. For example, an application for a payment service provider (PSP) license was denied on the basis of suspicion of ML after extensive inquiries by BoS. During the application process BoS received information from a foreign a supervisor regarding a close family member of a qualifying holder of the applicant who previously held a management position with a company involved in activities that included ML. Based on this information BoS sought the opinion of the OMLP which determined that the operation of the applicant in Slovenia would seriously increase the exposure of the financial system to ML.

407. Another application regarding a PSP was rejected based on the lack of ML/FT controls. The company later received a licence to operate in another EU state and although the licence limited its operation to that state alone the company stated offering their services in Slovenia. The BoS informed the foreign supervisor.

408. MVTS are offered by two international companies through Slovenian banks. The assessment team was informed by the BoS and MIRS that they intend to operate in the future through an independent agent outside of a bank but during a meeting with an obliged entity it was discovered that they started operating during 2016 without the knowledge of authorities. This raises concern about the ability of competent authorities to detect entities that operate without the required license.

409. Exchange offices are not licensed and are therefore not vetted regarding ownership or control by criminals or their associates, but they are supervised by BoS and all employees must pass knowledge exams.

DNFBPs

410. Lawyers, notaries and auditors who must be licensed have to show they have no convictions and a good reputation however in practice only criminal convictions are checked. In one case presented to the assessment team a lawyer that was suspected of fraudulently obtaining funds and laundering the proceeds did not have his license revoked until he was convicted.

411. It is widely recognised in various jurisdictions that casinos are prone to ML/FT risks and involvement of organised crime and it is therefore a concern that owners are subject only to criminal conviction checks. The FARS regularly seeks illegal internet casinos that operate in Slovenia and block their URL, but the ease of resuming operation under another address raises questions regarding the effectiveness of these measures.

412. Real estate agents that are natural persons must register with the Chamber of Real Estate and have to show that they have no relevant convictions. However, the MIRS have difficulty in obtaining information on the active agents as there is no central registrar that includes all agents.

413. According to the authorities there are no TCSPs operating in Slovenia. However public resources show that there are legal entities offering TSCP services.

414. Other DNFBPs such as tax advisors, accountants, traders in second hand gold and pawnbrokers are not required to be licensed and are not required to register with any professional association.

Supervisors' understanding and identification of ML/FT risks

415. The banking sector is by far the largest in the financial sector and the BoS, responsible for its supervision, has a good understanding of the ML risks in its supervision of banks and is aware of the prevalent typologies for ML in the national context as well as the methodologies prevalent in banks. The BoS was actively involved in the process of preparing the NRA.

416. BoS's knowledge of ML/FT issues is based on their ongoing dialogue with banks who provide them with updated information regarding new developments. However, the lack of regular and systematic sharing of information with the OMLP and with other supervisors hampers the collective understanding required to effectively identify ML/FT risks. The sharing of information could assist in better identifying and understanding of the risks involved in the use of the Bitcoin and other virtual currencies. For example, the assessment team was informed of a new trend, the use of Bitcoins to purchase gold in Slovenia, which was unknown to supervisors.

417. As previously mentioned, the BoS has good understanding of risks whilst other financial supervisors have a general understanding of the level of risks in their areas of responsibility they lack understanding at the product and customer level. During the interviews they had difficulty in discussing the specific risks in their sectors. At the same time during the interviews it was sometimes demonstrated that the obliged entities had a better level of understanding of specific risks than the supervisors. The BoS in its other supervisory functions (non-banking) and other financial supervisors could also benefit from a close dialogue with supervised entities who sometimes have more extensive knowledge regarding the ML risks in their sectors. With regards to FIs providing services under EU passporting regime there is a complete lack of information by the supervisors regarding the scope of their activities in Slovenia and it is therefore not possible to assess the risks associated with this activity. This shortcoming regarding credit institutions was recognized in the NRA and was addressed in the AML/CFT Action Plan adopted by Slovenia.

418. There are about 300 FIs (other than banks) from EU countries[61] whose supervisors have notified the Slovenian authorities of their intention to provide services directly or via branch in Slovenia but despite efforts made by the BoS vis-à-vis the relevant foreign supervisor, there is no information regarding their activity in Slovenia. As regards MVTS operating extensively via a non-banking representative, under an EU passport, the BoS was unaware of their activity even though they were notified by the foreign supervisor of the intended activity about a year ago. The lack of knowledge regarding these activities makes it impossible to assess the risks associated with these activities.

419. Despite the fact that the supervisors of DNFBPs, where they exist, were involved in the preparation of the original NRA, during the interviews they displayed a low level of understanding of ML/FT risks, with the exception of FARS.

420. With regards to FT risks there is an across the board agreement amongst all supervisors and professional bodies that much needs to be done to improve their knowledge of risks in this area.

421. The new APMLFT, which came into force during the on-site visit, provides the OMLP the authority to directly supervise obliged entities and conduct on-site inspections. The OMLP has not yet recruited the additional staff that will be responsible for supervision and has not conducted a risk assessment of the areas that they are now responsible for.

Risk-based supervision of compliance with AML/CTF requirements

Supervisors of Banks, Insurance and Securities companies

422. The BoS has two well informed staff members committed full time to supervising banks with regards to AML/CTF issues. As of 2013 the BoS sends an annual questionnaire to all banks. Based on this information and external inputs, such as media and results of previous inspections, an ML/FT risk matrix is prepared. Each bank is assigned a risk rating composed of the assessment of the bank's inherent risks and the quality of its internal controls. The inherent risk rating takes into account factors such as the bank's structure including its subsidiaries, the products and services they offer and the type of clients (with this regard a gap exists as BoS collects data on foreign entities but not on the number and activity of domestic legal persons with foreign ownership), which allows to account for the risks identifies in the NRA as well as other risks recognized by BoS. The system of internal controls rating takes into account the role of AML compliance officer, internal controls like AML/CFT internal policies and procedures, internal reporting, IT system, role of internal audit, information gained from previous supervisory activities and other relevant information.

423. The AML/CFT risk rating of a bank determined by the risk based methodology which has been adopted in 2014 determines not only the quantity and scope of ML/FT inspections but also has a direct impact on BoS's requirements concerning the robustness of the AML/CFT system in the bank. Although the risk based approach is in operation for some time the relevant procedure is still in draft form and BoS is awaiting the issuing of EBA guidelines before formally adopting the procedures.

424. The following table shows the number and types of AML/CFT on-site inspections conducted in banks from January 2010 – March 2016

Table 17: **AML/FT on-site inspections conducted in banks since January 2010 – March 2016**

Year	Full-scope	Follow-up	Targeted	Thematic	Total

[61] With respect to the supervision of passported FIs (other than banks) under the current EU framework, the home supervisor is responsible for the AML oversight of the authorised FI operating under the free provision of services. In that case, should the host supervisor become aware of concerns about the AML/CFT compliance in its territory, it should inform the home supervisor who can take the adequate action to address the shortcomings, including by delegating supervisory powers to the host authority. When an FI operates under the freedom of establishment in the host country, AML supervisory competences belong to the host supervisor. The 4th EU AML Directive is expected to further strengthen the cooperation.

	inspection	inspection	inspection (specific issue within a bank)	inspection (a specific issue inspected in a range of banks)	
2010	5	1	2	1	9
2011	3	7	0	0	10
2012	1	6	0	0	7
2013	3	2	0	0	5
2014	1	4	1	0	6
2015	1	2	3	0	6
2016 (up to March)	0	2	0	0	2
Total	**14**	**24**	**6**	**1**	**45**

425. It is evident from the table, in the years 2010-2013 BoS was focused on full scope inspections and follow-up inspections intended to ascertain whether banks have adequate internal controls. Following the adoption of the risk based approach in 2014, targeted inspections were conducted in 2015. Onsite inspections always include the review of at least 50 customer files. During these reviews supervisors check the documentation of the CDD process and analyse the activity in the account. One of the purposes of the inspections is to influence banks to become more critical of transactions with no apparent economic justification. The level of inspections is adequate considering the size of the banking sector and the level of compliance prevalent in the sector.

426. Although the BoS consults the OMLP before every specific on-site inspection the effectiveness of the risk analysis of banks by BoS could be improved if they regularly receive information from the OMLP regarding the quality of STRs and CTRsof all banks.

427. Some Slovenian banks are subsidiaries of foreign banks from EU countries and there are Austrian banks with branches' subsidiaries in Slovenia. The BoS has cooperated with the Austrian supervisor regarding inspections they have conducted in banks that are Austrian subsidiaries and in branches of Austrian banks and both supervisors have held joint discussions with these banks with the aim of improving their AML/CFT compliance.

428. Only one Slovenian bank has subsidiaries abroad and the BoS has conducted an inspection in foreign subsidiaries in the Balkan region in cooperation with the local supervisor.

429. The SMA conducts specialized AML/CFT on-site inspections in brokerage and asset management firms. The five staff members who conduct inspections devote about 5% of their time to ML/FT issues and even less to the inspections themselves. The SMA has implemented a risk assessment of firms and bases the frequency of inspections on this model, whose risk factors are not connected to ML/FT risks. Inspections conducted by the SMA are comprehensive and technical in nature and they are less focused on effectiveness. There are no targeted or thematic inspections. The SMA has raised some doubts about the quality of CDD that is conducted by tied agents; however this issue is not covered by their inspections. The overall number of inspections in the securities sector is adequate considering the materiality of the sector, but the fact that the SMA does not implement a risk based approach to AML/FT inspections hinders the effectiveness of these inspections.

430. The SMA has previously conducted inspections in banks regarding securities activity. With the new APMLFT in force they also have the authority to address ML/FT activities related to securities activity in banks although it is not clear how this will be done. In the past there have been cases of cooperation between the SMA and the BoS on specific issues but the SMA has conducted its inspections in banks without informing the BoS. If the SMA decides to use their new powers in banks it is desirable that this is done in close coordination with the BoS.

431. The ISA has two staff members who are responsible for ML/FT issues. They devote only between 400-450 hours annually to ML/FT issues. On-site inspections in this area are aimed at checking the compliance with all requirements of the law and no risk based approach has been adopted in these inspections. As with the securities sector, the number of inspections in the insurance sector is adequate but their effectiveness is hindered by the lack of a risk based approach.

432. The staff in the BoS, ISA or SMA has gained their relevant ML/FT knowledge "on the job" – no formal training has been conducted for the relevant supervisory staff.

433. The number of staff members devoted to AML/CFT supervision in the banking, securities and insurance sectors can be adequate if SMA and ISA adopt and implement a risk based approach to AML/CFT supervision and undergo specific ML/FT training.

Other financial institution supervisors

434. Other financial institutions are supervised by the MIRS (loan agencies) or the BoS (e-money institutions, payment institutions and money exchange offices), which has conducted inspections in many of the entities under its supervision. It was unclear during the on-site who is responsible for the supervision of MVTS operating through one agent outside of banks. The MIRS and the department in the BoS that is responsible for supervising the entities mentioned in this paragraph have no resources exclusively dedicated to ML/FT issues and their inspections include these issues as an additional subject to their main objective of safe and sound business and consumer protection. The MIRS has 25 supervisors responsible for a wide range of institutions and the enforcement of over 50 bylaws. The resources that can be applied to ML/FT issues are therefore extremely limited.

435. As previously mentioned FI's and MVTS operate in Slovenia under EU passporting regime without any supervision of a Slovenian supervisor and without any supervisory contact with the EU home supervisor. It is a concern that these institutions are not supervised regarding their activities in Slovenia.

DNFBPs supervisors

436. The FARS, responsible for supervising casinos, gaming halls and lotteries has 10 inspectors that also inspect ML/FT issues on-site. In addition, the FARS also has access to databases, which enables a good level of offsite supervision of online gambling. The supervision is not risk based.

437. Lawyers are supervised by the Bar Association who does not apply a risk based approach. Their AML/CFT supervision is based on a self-assessment questionnaire sent to lawyers with a response rate of about 25%. No risk based approach is applied.

438. The chamber of notaries conduct combined inspections that include ML/FT issues and they do not apply a risk based approach.

439. The MIRS responsible for supervising real estate agents and loan agencies base their inspection plan on previous findings with regard to consumer issues. Inspections include ML/FT issues.

440. The rest of the DNFBP sectors have a very low level of supervision. In the case of loan agencies, tax advisors, accountants, traders in precious metals and real estate agents the lack of information regarding the persons operating in these areas makes effective supervision impossible. This is especially concerning with regards to the relatively high-risk areas of trading in used gold and real estate agents.

441. Despite the high risk associated with dealers of precious metals, they were not supervised in Slovenia regarding their compliance with the APMLFT.

OMLP Supervision

442. In addition to the inspection powers of other supervisors, the OMLP has independent authority to supervise obliged entities off site. Although they recognise that certain sectors are under-supervised in relation to the risks they have not used their power for lack of resources and under the assumption that offsite inspections are not effective. The new APMLFT extends the OMLP's authority to conduct on-site inspections in the premises of obliged entities. The OMLP plans to recruit three additional staff members to fulfil this function but has not yet started the process and although it is aware of the need to develop a risk based supervision strategy this has not yet begun. APMLFT contains in Article 155 a provision on national cooperation between supervisory authorities and obligates supervisory authorities to make efforts to ensure the effectiveness of measures and supervision in combating money laundering and terrorist financing.

443. The OMLP has in rare cases (7 cases in 6 years) initiated inspections by other supervisors which have targeted specific problems but there is no regular exchange of information which could assist supervisors in assessing the risks of particular obliged entities.

444. The following Table 17 shows the number of inspections conducted by all supervisors and those dedicated to ML/FT issues:

Inspections in the period 2010-March 2016				
	Total number of entities as of 31 Dec 2015	**Total number of on-site visits conducted**	**Number of AML/CFT specific on-site visits conducted**	**Number of AML/CFT combined with general supervision on-site visit carried out**
	1	**2**	**3**	**4**
FINANCIAL SECTOR				
Banks	**23** **Banks (16)** **Saving houses (3)** **Branches (4)**	**45**	**37** **Full-scope (8)** **Follow-up (22)** **Targeted (6)** **Thematic (1)**	**8** **Follow-up (2)** **Full-scope (6)**
Securities	**5**	**6**	**1**	**5**
Insurance	**18**	**32**	**-**	**24**
Exchange offices	**24**	**130**	**0**	**130**
Payment institutions	**4**	**9**	**1**	**5**
E-money institutions	**1**	**1**	**0**	**0**
Management Companies	**9**	**11**	**9**	**2**
Investment	**10**	**-**	**-**	**-**

Pension Funds				
NON-FINANCIAL SECTOR				
Casinos	**10+27=37**	**1094**	**1**	**823**
Real estate	**223***	**260**	**260**	**260**
Dealers in precious metals and stones	**80**	**-**	**-**	**-**
Lawyers	**1684** (on 31.12.2015)	**209**	**-**	**-**
Notaries	**93**	**58**		**58**
Accountants & Auditors	**54 audit Firms** **4.431 accountants**	**57** (+1 additional inspection conducted directly by the Agency)	**0** The Agency issued 1 order to 1 audit firm to improve the AML procedures	**20** (+1 additional inspection conducted directly by the Agency)

* Members of the Chamber of Real Estate

Remedial actions and effective, proportionate, and dissuasive sanctions

Bank of Slovenia

445. The following Table 18 shows the supervisory measures applied by the BoS following breaches that were detected during inspections, in the years January 2010 - March 2016:

Year	**Total number of inspections conducted**	**Number of inspections where breaches were identified**	**Supervisory measures**	**Misdemeanours (fines)**
2010	**9**	5	Letter with admonishments (4) Order on the rectification of breaches (1)	0
2011	10	7	Letter with admonishments (1) Order on the rectification of breaches (2+2) Order with additional measures (2)	0
2012	7	3	Order on the rectification of breaches (1+1) Order with additional measures (1)	0
2013	5	2	Letter with admonishments (1) Order on the rectification of breaches (1)	0
2014	6	3	Letter with admonishments (1) Order on the rectification of breaches (1+1)	0
2015	6	1	Order on the rectification of breaches (1)	0
2016	**2**	**1**	Order with additional measures (1)	
Total	**45**	**22**		**0**

446. The impression of the assessment team from interviewing the BoS and individual banks is that in many cases the measures undertaken by the BoS following the detection of breaches has been effective. However, in cases of repeated or systematic breaches by banks, financial sanctions were not imposed even though they would have had an additional positive effect on the level of compliance. The process of imposing financial sanctions is lengthy and is dependent on legal resources that are not prioritised for this matter. This raises the question if the framework for sanctions as a whole is in fact fully effective. The BoS has never imposed financial sanctions on a bank for breaches of the APMLFT.

447. The BoS has also not used its power to revoke the licence of a member of the board, on the basis of AML/CFT breaches. There was one case where systematic breaches were identified in the AML/CFT area in one bank which were attributed to a particular member of the board and BoS considered using its power to revoke the licence for the member of the board responsible also taking into account other relevant information from prudential supervision. Finally, no such action was necessary as the relevant board member resigned; however the board member can be subject to financial sanctions and no decision has been reached in this regard.

448. The BoS does not have the power to remove the AML compliance officers from their position but there have been cases where banks replaced compliance officers after the BoS imposed measures following an inspection.

All Supervisors

449. The following Table 19 provides a summary of sanctions and other measures used by all supervisors following infringements found during inspections:

1.1.2010-31.3.2016									
	Total number of inspections carried out	**Number of inspections having identified AML/CFT infringements**	**Type of sanction/measure applied**						**Number of sanctions taken to court**
			Written warning	**Fines**		**Removal of manager/compliance officer**	**Withdrawal of license**	**Other**	
				Number	**Amount (EUR)**				
FINANCIAL SECTOR									
Banks	**45**	**22**	22 (see Table 18 for detailed information)	**-**	**-**	**-**	**-**	**-**	**-**
Securities	**6**	**3**	**3**	**-**	**-**	**-**	**-**	**-**	**-**
Insurance	**24**	**8**	**3**	**1**	**-**	**-**	**-**	**-**	**-**
MSBs and exchange offices	**35**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Payment institution	**9**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

s									
E-money institutions	**1**	**0**		**-**	**-**	**-**	**-**	**-**	**-**
Creditors	**178**	**84**	**78**	**1**	**-**	**-**	**-**	**-**	**-**
Pawnshops	**13**	**6**	**6**	**-**	**-**	**-**	**-**	**-**	**-**
Management companies	**11**	**4**	**6**	**1**	**-**	**-**	**-**	**9 (recommendation)**	**-**
Investment Pension Funds	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
NON-FINANCIAL SECTOR									
Casinos	**1092**	**6**	**6**	**3**	**1251**	**-**	**-**	**25.600**	**-**
Real estate	**260**	**115**	**115**			**-**		**1 (minor offence decision)** **1**	
Dealers in precious metals and stones	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Lawyers	**209**	**80**	**-**	**-**	**-**	**-**	**-**	**3 (recommendation)**	**-**
Notaries	**38**	**29**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
Accountants & auditors	**52**	**29**	**29**	**2**	**950**	**-**	**-**	**-**	**-**

450. It is evident from the data that severe sanctions such as financial sanctions, withdrawal of license or removal from a management position are rarely imposed even though they are enabled by the legislation. It is understood from the interviews that on the whole, supervisory measures achieve rectification of the breaches and dissuade obliged entities from further breaches; however the use of more severe measures should be considered. BoS has recognised the shortcoming of the lack of financial sanctions and following their recommendation the action plan adopted by the government has given priority to this issue.

Impact of supervisory actions on compliance

451. The BoS has been able to demonstrate a significant improvement in the level of AML/CFT compliance of banks under its supervision. Before 2010 banks were mostly focused on formally fulfilling legal requirements. Partly as a consequence of BoS's actions (issuing guidance, dialogue

with the banks, on-site supervision and subsequent supervisory measures), management of banks has improved their commitment to mitigating AML/CFT risk which has led to the strengthening of the AML compliance functions in banks. For example in many banks AML compliance officers are now considered a 'key function' and the AML compliance function which was in the past usually comprised of one person has increased, in one bank to a five person team.

452. Thematic workshops for banks that elaborated on every phase of suspicious transaction reporting had a positive effect on the reporting habits of participating institutions.

453. The lack of the use of financial sanctions is likely to hamper the BoS's efforts to further improve banks commitment.

454. The interviews with banks strengthened the impression that the BoS's actions are having a positive impact on their compliance. Interviews with brokerage and asset management companies also indicated that the SMA has a positive effect on their commitment to compliance. However, the perceived 'tough' approach and attention to detail by the supervisor has also had the effect of causing obliged entities to give technical matters disproportionate attention. Interviews with insurance companies indicate that their compliance functions are active in achieving compliance with their obligation under the APMLFT.

455. As regards other FIs and DNFBPs it was not demonstrated that supervisors, as far as they exist, have a positive effect on the compliance with AML/CFT obligations by obliged entities.

456. Overall there is no systematic measurement of compliance levels in obliged entities by supervisors.

Promoting a clear understanding of AML/CTF obligations and ML/FT risks

Guidelines and ongoing guidance

457. The OMLP has initiated the publication of guidelines for the various sectors on their own (dealers in precious metals, credit institutions, accountants and real estate agents) or in collaboration with the competent supervisors. There is an understanding amongst supervisors and the OMLP that there is a need to update these guidelines that are mostly over five years old and the assessment team has been informed that this will be done after the amendments to the law comes into force.

458. The BoS has also issued circular letters pointing out the latest updates in AML/CFT area. The last circular was issued in August 2016 and included topics such as accounts of asylum seekers, Iran and ML typologies.

459. Interviews with obliged entities have shown that the guidelines alone, reaching up to 100 pages in length, are ineffective in increasing their knowledge and understanding of ML/FT issues unless combined with inspections and training activity. Interviews with professional associations have shown that even they are not always conversant with the contents of the guidelines, and that most supervisors are not aware of the FT indicators included in the annexes.

460. The OMLP is active in promoting understanding of AML obligation in the different sectors through its regular responses to questions that arise from the various entities that often prefer to ask their opinion in relation to ML/FT issues rather than their competent supervisor. The answers are usually provided by the OMLP without consultation or coordination with the direct supervisor and the assessment team has been informed that there are some cases where the supervisors and the OMLP have different views. Sharing this process with the supervisors can enhance certainty and the overall level of understanding by the supervisors.

461. One of the banks interviewed made a positive referral to the feedback that its compliance function receives in meetings with the OMLP dedicated to discussing the quality of the reports. It may be desirable to include supervisors in these meetings or at least inform them of their content.

Training

462. In the last five years training has been focused on banks, securities companies and exchange offices. Training is conducted by representative associations (banking, stock exchange members and asset managers) with assistance from the OMLP. Supervisors participate in these trainings but do not initiate them.

463. With regards other FIs and DNFBPs the only seminars conducted in conjunction with the relevant associations were for notaries, auditors and accounting services and these were last conducted in the years 2011-2014.

464. All the seminars but one that have been conducted were exclusively focused on ML issues and the first seminar dedicated to FT issues was conducted for banks in October 2016. The BoS was not invited to participate in this seminar.

465. The OMLP recognises that the efforts made are not sufficient to achieve a high level of understanding by obliged entities and is of the opinion that more should be done to improve the understanding of the non-banking financial sector and to reach out to DNFBPs despite the difficulties involved (see comment in next section).

Other issues

466. BoS and OMLP issue circulars to provide obliged entities with an update regarding new developments. The circulars issued by the OMLP are also published on its website.

467. The large number of DNFBPs such as Accountants, Tax advisors and traders in precious metals that are not required to be registered, licensed or members of any association pose a serious challenge for the OMLP in reaching and educating them regarding their obligations. There are still many OE's that are uninformed especially amongst DNFBP's.

468. Efforts to date have concentrated on understanding ML with little regard to FT issues. The supervisory authorities are aware of this deficiency and intend to pay more attention in future to understanding FT issues.

Overall Conclusions on Immediate Outcome 3

469. The supervisors of banks, insurance companies, securities firms, e-money and payment institutions have the authority to refuse or revoke a licence based on 'fit and proper' concerns with respect to owners and managers. In practice the supervisors conduct checks based on comprehensive questionnaires and searches that include publically available information and, on occasion, confidential information received from foreign supervisors. There is a concern that the current regime is not sufficient in preventing persons with criminal background and their associates from controlling obliged entities. In the DNFBP sectors some require no licensing and in cases where licenses are required (lawyers, notaries, real estate agents and casinos) the application can be refused or a license revoked only on the basis of a criminal conviction.

470. Key financial supervisors (BoS, ISA and SMA) regularly conduct on-site inspections in banks, insurance companies and securities firms but only the BoS use a risk based approach based on ML/FT parameters in planning their inspections and overall supervision. The other supervisors do not base their supervision on ML/FT risks and this means that their limited resources assigned to ML/FT issues are not used effectively.

471. The law empowers supervisors to impose a wide range of sanctions on obliged entities for breaches of their obligations under the APMLFT, but the more severe sanctions are very rarely used. This raises questions regarding the dissuasiveness of sanctions as a whole with special reference to the DNFBP sector where the amount of inspections is very low or non-existent including in areas of high risk such as real estate. It is expected that the number of inspections in the sectors that have been identified as higher risk will increase when the OMLP starts to implement its newly acquired inspection powers.

472. As regards financial services operating in Slovenia under EU passporting rules there have been no inspections by Slovenian or home supervisors.

473.Outreach efforts by supervisors include written guidance and specific training targeted to certain sectors but more efforts needs to be made to make obliged entities aware of the risks in their sectors and their obligations under the law. This is especially true with regards to all sectors outside the banking, insurance and securities sectors. Guidance related to FT risk is missing in all sectors.

474. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key Findings

1. Slovenia has not carried out an in-depth analysis of ML/FT vulnerabilities of all types of legal entities that may be established in the country, but the competent authorities have demonstrated an understanding of general vulnerabilities.

2. Basic information on legal entities established in Slovenia is publicly available via the Business Register. However, there are some concerns about the effectiveness of existing mechanisms to ensure that this information is accurate and up-to-date.

3. Slovenia has certain mechanisms in place to prevent the misuse of legal entities. Prospective founders, shareholders and managers of legal entities are subject to criminal background checks, and restrictions were recently imposed on the number of companies that can be set up by one person. However, these measures have not proven sufficient to effectively counter the commonly observed ML typology of abusing shell companies via straw men.

4. Competent authorities rely on obliged entities to obtain the beneficial ownership information. Difficulties identified in relation to the verification of beneficial owners by obliged entities suggest that reliable beneficial ownership information may not always be available. Notaries and other DNFBPs involved in setting up legal entities do not adequately fulfil their gatekeepers' role. However, the overwhelming majority of companies have accounts opened in Slovenian banks, which demonstrated a much better compliance with beneficial ownership requirements

5. The new APMLFT requires legal persons to obtain their beneficial ownership information and report this to the central beneficial ownership registry once it is created. There are however concerns as to whether the OMLP will have the capacity to adequately verify the accuracy of information intended for the registry.

6. The Slovenian legal framework does not recognize trusts, although the operation of legal arrangements established under foreign law is not prohibited. The assessment team was not convinced that authorities or obliged entities are adequately aware of ML/FT risks related to legal arrangements as they lack understanding of their structures and the nature of their activities.

Recommended Actions

Slovenia should:

1. Conduct an in-depth assessment of vulnerabilities and potential for ML/FT abuse of all types of legal persons that may be established in the country, and take coordinated measures to effectively mitigate the risks.

2. Provide guidance and implement respective supervisory measures to ensure that notaries and other DNFBPs involved in the setting up of legal persons apply CDD measures effectively and are able to identify potential abuses of legal entities.

3. Implement measures to ensure that nominee shareholders and directors are not misused (consideration could be given to introducing the mechanisms suggested under R.24.12(a) and (b)).

4. Strengthen the existing oversight procedure to ensure that basic information on legal persons held in the Business Register is accurate and up-to-date, and that effective, proportionate and dissuasive sanctions are applied for breaches of reporting requirements.

5. Ensure in relation to the newly introduced mechanism for obtaining beneficial ownership information that the OMLP will be provided with sufficient tools and resources to ensure that the information is accurate, up-to date and available to competent authorities in a timely manner. Slovenia may also consider giving sufficient powers to legal persons to require the disclosure of their own beneficial ownership information from partners, shareholders or other relevant parties, and to take adequate action when they fail to do so.

6. Require trustees of foreign trusts and equivalent persons in other legal arrangements to disclose their status when doing business with obliged entities.

475. The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The recommendations relevant for the assessment of effectiveness under this section are R.24 & 25.

Immediate Outcome 5 (Legal Persons and Arrangements)

Public availability of information on the creation and types of legal persons and arrangements

476. Information on the creation and types of legal entities in Slovenia is available through various legal acts regulating state registers and different legal entities. There is no single act describing all possible types of legal entities that may be established in Slovenia. Information on registered legal entities is available on-line on the website of the Agency of the Republic of Slovenia for Public Legal Records and Related Services (APLRRS). APLRRS manages the Slovenian Business Register, which includes different primary registries for legal persons and is publicly available upon the creation of an account. Some summarized information on the creation of certain types of legal entities is also available on the website of APLRRS.[62] The website of the Ministry of Interior provides such information for associations and foundations.[63]

477. As of 30th of September 2016, the Business Register contained information on 75,572 companies (commercial legal entities), 23,996 associations and 8,689 other types of non-profit organisations (e.g. foundations, trade unions, institutes), as well as 444 cooperatives (see also Table 3 in the Introduction chapter). The overwhelming majority of companies are limited liability companies (70,245). Furthermore, there are 737 unlimited companies, 705 public limited companies (joint-stock companies) and 379 limited partnerships.

478. The evaluators were not given data on how many companies are foreign owned. However, around 17% of limited liability companies, 7% of unlimited companies and 6% of limited partnerships have at least one shareholder with a foreign address. Moreover, 18 out of 292 foundations (6%) and 260 out of 2,243 institutes (12%) were founded by at least one foreigner (mostly from Austria, Italy, UK, Croatia and Germany). No similar statistics were provided for associations.

Identification, assessment and understanding of ML/FT risks and vulnerabilities of legal entities

479. Slovenia has not conducted a comprehensive assessment of ML/FT risks stemming from the characteristics, nature and scope of activities of various types of legal persons that exist in the country, but the NRAs contain relevant information to some extent. The NRAs consider the availability of information on legal entities in the context of implementation of CDD requirements by obliged entities as part of the national vulnerabilities assessment. They stress that online access to registries on legal persons and on bank accounts is of great assistance to banks in the process of verifying the data submitted by customers. At the same time, difficulties for banks in obtaining the beneficial ownership information on legal entities with foreign ownership are considered as a major vulnerability.

[62] www.ajpes.si.

[63] www.mnz.gov.si/si/mnz_za_vas/drustva_ustanove_shodi_prireditve/.

480. The NRAs also highlight the introduction of new search features in the Business Register since August 2015 as a way to significantly improve transparency and help obliged entities verify business activities of their customers. In particular, the addition of a “people search engine” to the Business Register makes it possible to find out if a particular person is the founder, partner, representative or member of the supervisory board in a legal entity.

481. Another issue considered in the NRAs is the possibility for a natural person to establish multiple companies without limitations, which could be abused for ML or other economic crime purposes. Amendments introduced to the Companies Act in January 2016 sought to address this issue (see further below under ‘Mitigating measures’). The NRAs however do not address the vulnerabilities related to the recently introduced “one stop shops” that provide a quick and easy procedure of setting up certain types of companies; or the limited application of CDD measures by notaries and other DNFBPs when relatively complex legal entities are created.

482. The NRAs contain some information on criminal proceedings against legal persons in the context of offences related to business fraud and abuse of position of trust. However, this falls short of comprehensively analysing threats associated with the use of different types of legal entities from the perspective of serious economic and other crime both in the domestic and cross-border context, and the adequacy of existing countermeasures. The NRAs also include a limited analysis of the adequacy of legislation on foundations, institutes and associations, but fail to consider the vulnerabilities and potential for misuse of NPOs in the ML/FT context.

483. Although ML/FT risks related to legal persons were only partially analysed within the NRAs, several competent authorities interviewed on-site did demonstrate further awareness of risks. Complex legal structures involving foreign legal persons and offshore bank accounts were mentioned most commonly. Another practice that competent authorities (OMLP, FARS, Police, prosecutors) often identify relates to the use of shell companies and the involvement of (foreign) straw men. The assessment team was also informed on the establishment of legal entities by foreigners for the purposes of opening accounts in Slovenian banks and buying real estate. However, some interlocutors saw this as an attempt to circumvent domestic restrictions on foreign ownership of real estate rather than an indication of ML. Authorities responsible for company registration also mentioned risks of abuse of legal entities established with real estate property as their founding capital.

484. Regarding cross-border risks, in 2016, the OMLP performed an analysis of inflows and outflows through banks of over EUR 5,000 from and to a list of offshore jurisdictions with special focus on transactions of resident companies. The methodology included checks in the Slovenian Business Register to identify transfers performed by companies owned by the state and those with direct foreign ownership. Attempts were made to establish links between the companies’ owners and representatives with persons included in databases of the OMLP and LEAs. According to the OMLP, most offshore transfers could be explained on the surface as legitimate business activities, but some discrepancies gave rise to further inquiry.

485. At the time of the on-site visit, the OMLP was working on a strategic analysis of cross-border incoming and outgoing bank transfers as a continuation of the aforementioned exercise. This included a closer look at transactions between Slovenian and foreign companies to identify typologies of potential abuse. Some preliminary results indicating countries warranting increased focus and abusive practices related to predicate offences were shared with the evaluation team during the on-site interviews.

486. The OMLP has identified the practice of nationals of a neighbouring country laundering proceeds of tax evasion via establishing legal entities and opening bank accounts in Slovenia (Country X typology, see IO.6 and 7). It has sent out a circular letter explaining the typology to all banks that subsequently demonstrated a more careful approach in establishing business relations with such entities in the absence of clear reasons for doing business in Slovenia. The OMLP has

further observed Slovenian citizens to be behind ML schemes involving shell companies and using citizens from neighbouring countries as intermediaries.

487. As explained in more detail under IO.10, intelligence and law enforcement authorities met on-site were also aware of possible misuse of NPOs for FT purposes.

488. The evaluation team believes that the awareness of the risks of abuse of legal persons could be further improved and integrated among competent authorities. The team observed that not all authorities which could play an important mitigating role had sufficient knowledge or expertise to understand and help prevent the misuse of legal persons. Furthermore, authorities did not always have a uniform or in-depth view of typologies, nor did they appear to exchange information that could support mutual understanding. The assessment team was also not convinced that authorities are aware of ML/FT risks related to legal arrangements (foreign trusts) that can operate in Slovenia, since they did not demonstrate a proper understanding of their structures and the nature of their activities.

Mitigating measures to prevent the misuse of legal persons and arrangements

489. There are several factors that lower the risk of misuse of legal entities in Slovenia. The country has a strong tradition of ensuring transparency of legal ownership. Basic information on legal entities is publicly available through the Business Register, which incorporates information from various state registries and appears to be adequately managed by APLRRS. The information contained in the registry is divided into publicly available on-line information (subject to simple registration on the web-site of APLRRS) and information made available to the public upon request or to competent authorities when certain legal grounds are met.

490. In general, the evaluation team notes that the Business Register contains useful information and serves as basic reference for obliged entities, who expressed satisfaction with the availability and reliability of the information provided. The aforementioned recent introduction of the "people search engine" feature within the Register is an important improvement of transparency. However, evaluators have some concerns about the reliability of the data contained in the registry (see core issue 5.6).

491. Information on the shareholders of public limited companies is accessible to the public through the central registry of dematerialized securities maintained by the Central Securities Clearing Corporation (CSSC) based on the Book Entry Securities Act. Transfers of shares are conducted via the central registry and are only valid once reflected there. The data from share books, such as the holder's name, address, country of residence and quantity of shares held is publicly available online, while the data on the nature of associated voting rights can be retrieved from the Business Register.

492. The existing registry system has a number of safeguards in place to prevent the misuse of companies. As required by law (Art. 10a Companies Act), all natural and legal persons, including non-residents, who apply to become founders or shareholders of a company are checked against lists provided by the Ministry of Justice and the Ministry of Finance (see below) both in the process of establishing a company and later, when changes among shareholders occur. If there is a hit, the application for the registration of a company or a new shareholder will be rejected. Legal representatives and directors of companies are also checked against the lists (Art. 10a, 255, 515 Companies Act). However, while the validity of changes in shareholding depends on their successful registration, appointment of a new legal representative or director is valid from the moment of shareholders' decision. Thus, the legal consequences of rejecting the registration of changes in legal representatives or directors of existing companies are not entirely clear.

493. The list of the Ministry of Justice contains (domestic or foreign) persons that have been convicted for offences against the economy, employment and social security, legal transactions, property, environment and natural resources. Since the list only contains foreign persons as far as they were convicted in Slovenia, a notarised foreign founder's or shareholder's statement on the absence of convictions in the country of residence is also required. In case of foreign legal persons establishing a company in Slovenia, such statements must be provided both for the legal entity and

its representative. The list of the Ministry of Finance contains (domestic or foreign) persons that failed to submit their financial statements or to make public their list of tax defaulters on the basis of the Tax Procedure Act.

494. The registering authorities further check whether all required documents for legal entities are provided. For public limited companies and limited liability companies, the required documentation includes bank certificates on the company's bank account and founding capital. Authorities advised that this does not amount to a requirement that a company must have a bank account in Slovenia – it can also be in another country. Legal persons also need to have a bank account for taxation purposes under the Tax Procedure Act, although FARS clarified that this can also be a foreign bank account. However, statistics on limited liability companies show that only around 300 out of more than 70,000 companies do not have a Slovenian bank account (less than 0,5%). The evaluators were not provided with similar statistics on other types of legal entities.

495. There are no national statistics available on the number of refusals to establish companies broken down by type or reason for refusal. The District Court of Ljubljana, which registers approximately 50% of all court-registered legal entities in Slovenia, reported that from January to September 2016, applications for registration were rejected for 35 limited liability companies (against 1,690 approvals) and 3 institutes (against 144 approvals). The evaluators could not ascertain whether any of these rejections were related to AML/CTF concerns.

496. There are concerns that DNFBPs, especially notaries, which play a key role in setting up of complex companies, do not properly fulfil their gatekeepers' role. Involvement of notaries is required by the Slovenian law when corporate structures within companies are arranged differently from standard legal provisions or subsidiaries of foreign companies are incorporated. Moreover, establishment of companies posing risks of abuse as indicated by authorities met on-site, including those where share capital is partially or wholly contributed in kind (e.g. real estate), is part of notaries' primary duties. They are also responsible for certifying transfers of shares or changes to partnership (shareholders) agreements. However, notaries met on-site demonstrated a limited understanding and application of CDD measures. Their awareness of beneficial ownership requirements is quite low and they do not seem to examine the intended nature of business relationship or the sources of funds of their customers. This raises concerns that notaries may be missing signs of abuses of companies.

497. All legal persons must submit annual financial reports to both FARS and APLRRS. If reports are not submitted, APLRRS verifies whether the legal entity is active by sending a warning letter to the registered address. This measure, which is primarily aimed at assuring the publicity principle regulated by law, also serves to uncover the existence of so called dormant (shell) companies that could be used *inter alia* as vehicles for ML/FT schemes. The evaluators were informed that in case of non-response, sanctions are imposed and/or liquidation procedures to remove the entity from the registry are commenced. According to the authorities, this happens quite often, which was confirmed by statistics provided to the evaluators.

498. Since January 2016, the Companies Act introduced certain restrictions on the establishment of legal entities. In particular, the same person cannot establish a second limited liability company within three months of incorporating the first, while a person with unpaid tax duties cannot set up a company at all. These restrictions do not apply to directors or persons acquiring shares in existing companies. The authorities interviewed on-site believe this to be an important mitigating measure against abuse. A Police representative claimed that the trend of using Slovenian "shell companies" for ML and other economic crime purposes has consequently slowed down. The lawyers met on-site also declared that the practice of setting up and selling so called "shelf companies" does not persist. However, the evaluation team considers that the mitigating impact of these restrictions should be assessed over time as pointed out in the NRAs.

499. In 2006, Slovenia introduced the "book-entry" form of ownership for shares of public limited companies. Although issuing bearer shares is still possible in Slovenia, they are dematerialised under

the Companies Act and the Book Entry Securities Act states that for a transfer of dematerialized shares to be valid it has to be registered in the central register of dematerialised securities. The main difference between "normal" shares and bearer shares lies in the availability of information on shareholders: personal data of holders of "normal" shares is publicly available, while such a data for holders of bearer shares can only be made available to competent authorities upon their request. The evaluators were informed that there are 25 bearer shares currently registered, but the number of the rest (if any) is not known. According to the authorities, bearer share warrants do not exist in Slovenia, since they cannot be issued under the current legal framework.

500. Issuance of bearer shares is not possible for other types of companies than public limited companies. All shareholders (members) of limited liability companies and unlimited companies must be identified by name and reported to the registering authorities when the company is established or changes in shareholding occur.

501. FARS takes certain measures to combat the misuse of legal entities for criminal purposes in the context of tax evasion. It screens all tax liable companies on a weekly basis using a special automated system, which includes more than 80 VAT-fraud indicators, to identify high-risk companies. Special mobile units are sent to the offices of identified companies to conduct further checks. Traders can be removed from the VAT register if abuse is established. Information exchange and cooperation with the Police and prosecutors takes place to pursue identified illegal activity in criminal proceedings (see IO.7).

502. The authorities have taken some limited measures to prevent the misuse of nominee shareholdings by lawyers, notaries and other persons providing custodian services, which is enabled for public limited companies and limited partnerships with share capital. The nominee status is disclosed to brokerage companies when the latter are requested to open special "fiduciary accounts". The nominee status is obvious from the type of account. There appear to be no disclosure requirements on the nominee if a nominee holds securities for a nominator without the intermediation of a brokerage company. The authorities advised that the shareholders' threshold reporting duty to listed public limited companies and to the SMA does include shares held indirectly through a nominee (Art. 105, 117-120, 134 FIMA), which could mitigate the potential for abuse. It must also be noted that the evaluators did not identify any examples or concerns regarding the misuse of nominee shareholding during the on-site visit.

503. The issue of nominee directors is not specifically addressed under the Slovenian law. The authorities claimed that every director has the duty of care towards a company and will be held liable if ensuing responsibilities are neglected. However, this would not prevent the existence of arrangements whereby one natural person formally acts as a director on behalf of another person. There are no restrictions that would limit the number of companies where one person may operate as a director. The recent amendments to the Companies Act limiting the possibility for the same person to be the *founder* of more than one company (see above) do not extend to directors. Although obliged entities are required to obtain details about natural persons controlling a legal entity that would normally include the nominating director, there is a lack of understanding of the concept of beneficial ownership, especially in non-banking sectors (see IO.4). FARS does include the number of times a manager is involved in companies as a risk factor in its automated system, but only to detect potential tax evasion cases by legal persons. The limited measures applied to prevent the misuse of nominee directors raise concerns given that the use of legal entities and related (foreign) straw men features in major ML cases described in the NRAs and has often been referred to by Slovenian authorities and banks met on-site.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal persons

504. The availability of basic information on legal persons appears to be at a high level (see R.24).The time limit for companies to report changes in the data is 15 days (Art. 47-48 Companies Act). However, evaluators are concerned that changes of directors and legal representatives may not

always be notified given the absence of serious legal consequences (see core issue 5.3) and lack of imposed sanctions (see core issue 5.6) for legal entities in case of failure to report.

505. Slovenia has taken various measures to ensure the timely access by competent authorities to basic information on legal persons. Information held in the Business Register that is not publically accessible, such as ID numbers of company representatives, is made available to competent authorities. Furthermore, competent authorities, including the Police, OMLP and supervisors, have direct access to the data kept in the Central Securities Register that is also not public and includes personal ID-numbers of all registered shareholders, and names and ID numbers of those holding bearer shares of joint-stock companies. Checks on the ownership of shares by persons under the investigation are conducted "almost by default" according to the Police. CSCC can undertake more complicated searches of data (e.g. ownership turnover during a certain period of time or ownership on a particular date) and provide such information upon request to authorities. The CSCC reported that in the period of 2010-2016, the Police and the OMLP retrieved data from the Register either directly or upon request 19,941 and 84 times respectively.

506. Information on founders (natural or legal persons) of NPOs (foundations, associations, institutes) that is not published online is available to competent authorities upon request. The registering authorities are legally required to provide the requested data to competent authorities within 15 or 30 days depending on the requested authority, but the response time is often much shorter. The Ministry of Interior in charge of registering associations (the most common type of NPOs) reported that in 2015-2016 it received and responded to 112 requests from different authorities regarding information that is not published online.

507. Competent authorities interviewed on-site indicated no problems in obtaining the information held by registering authorities.

Box 14: Civil confiscation

To start a financial investigation for civil confiscation proceedings (see IO.8), the prosecutor must determine that three pre-conditions are fulfilled:

1) suspicion that a person committed a crime listed in Art. 4 of Civil Forfeiture of Assets of Illegal Origin Act;

2) suspicion that at least 50.000 EUR of assets of illegal origin is involved;

3) assets are not connected to a crime for which a conviction took place.

The Public Prosecutor's Office reported on a criminal case against several persons for unlawful manufacture and trade of drugs, which ended in plea agreements. Some insignificant amounts of proceeds of crimes were taken from the main perpetrator, whereas it was obvious from house searches and other sources that his lifestyle did not reflect his legal incomes. In deciding whether to open civil confiscation investigation against this person, it was established that the second legal condition for such an investigation (see above) was fulfilled based on house searches and information obtained from the CSCC about the shares held by the person.

508. Beneficial ownership information is not checked by the registering authorities in the course of the registration process, which goes as far as identifying one level of ownership above the newly created legal entity. In cases where the beneficial owner is not the same as the legal owner, the beneficial ownership information can be retrieved from obliged entities. However, except for banks and some other FIs, understanding of and compliance with beneficial ownership requirements is quite low among obliged entities (see IO.4). DNFBPS, including notaries, lawyers, tax advisors and audit firms are involved in the process of establishing relatively complex companies. However, they do not seem to adequately fulfil their gatekeepers' role and claimed to rely on banks to do required checks, as well as on registering authorities and the Tax Administration (who are actually not supposed to identify beneficial owners).

509. In terms of context and materiality, more than 99% of domestically-incorporated companies have an account with Slovenian banks. Although certain problems with the depth of verification of beneficial owners have also been observed in relation to some banks, the banking sector overall has the most advanced understanding of beneficial ownership requirements and undertakes required checks in most of the cases (see IO.4). This is particularly true of larger banks that serve the majority of customers that are legal entities. The supervisory measures carried out by BoS in recent years against failures in banks to properly identify beneficial owners (see core issue 5.6) appear to have led to significant improvements.

510. Thus, the availability and accuracy of beneficial ownership information in Slovenia seems to be ensured to a considerable extent. Competent authorities also did not report problems in retrieving the necessary data on beneficial ownership from banks, which was described as a regular practice. However, they also advised that in case of investigation of more complex schemes involving movements of funds between multiple domestic and foreign (shell) companies, identifying beneficial owners gets more complicated and often requires international cooperation, which is not always successful (see IO.2).

511. The APMLFT introduced new obligations for business entities in relation to ascertaining their own beneficial ownership, which are analysed in detail under R.24. However, the effectiveness of this measure could not be evaluated since business entities were given time until November 2017 to discover information on their beneficial owners, and until January 2018 to enter the information in an envisaged central beneficial ownership register. Authorities voiced some concerns as to whether appropriate measures will be taken to ensure that the beneficial ownership information intended for the registry is accurate and up-to-date. It was not yet clear during the on-site visit what powers would be given to legal entities to collect accurate information. Although the OMLP (the envisaged competent authority) was given the power to impose sanctions on legal entities for the failure to provide accurate beneficial ownership information, it was also not clear what mechanisms and resources will be made available to the OMLP to effectively enforce the new obligations.

Timely access to adequate, accurate and current basic and beneficial ownership information on legal arrangements

512. Trusts cannot be formed under Slovenian law. Yet there are no provisions precluding trusts or similar legal arrangements established under foreign law to conduct their activities through the Slovenian financial system, and no prohibitions for persons under the jurisdiction of Slovenia to act as trustees (or equivalent). Trust and company service providers (TCSPs) are obliged entities under the APMLFT; however the authorities claimed that no businesses or individuals provide trustee services in Slovenia. The evaluation team has not come across any information suggesting otherwise, although it did identify websites of businesses offering company (but not trust) services in Slovenia (e.g. providing registered address, see IO.3).

513. Authorities have advised that information on trusts and similar legal arrangements established under foreign law can be gathered through obliged entities implementing CDD procedures. Banks met on-site have observed such legal arrangements in complex ownership structures of their corporate clients, but in rare cases. It appears that all obliged entities, including banks, lack understanding of trust-like legal arrangements (see IO.4), which can lead to trustees using the Slovenian financial system undetected. There is also no obligation for trustees to disclose their status to obliged entities. Thus, there are concerns that competent authorities may not have timely access to the beneficial ownership information on legal arrangements.

514. As noted under IO.4 and R.25, the new APMLFT introduced more detailed requirements on the identification of trustees, settlors and beneficiaries of trusts, which could help clarify the obligations of obliged entities. Furthermore, business entities, which include trusts that have tax liabilities in Slovenia, are now required to collect and maintain records of their beneficial ownership and pass this information to the central beneficial ownership register. However, given the recent entry into force of the new APMLFT, the evaluators could not assess the effectiveness of these measures.

515. The evaluation team identified a Slovene type of legal arrangements, namely mutual investment funds (a form of UCITS funds), that are operated by management companies (see R.25). There are some mechanisms in place to ensure that accurate and up-to-date basic and beneficial ownership information is available on the mutual funds. Management companies are supervised by the SMA and must always keep the relevant information on investors. The SMA did not report any difficulties in obtaining the updated data on investors. As obliged entities under the APMLFT, management companies must identify and verify the identity of customers and their beneficial owners. This information can be requested both by the SMA and the OMLP. However, there are some concerns about the depth of verification of beneficial owners by management companies (see IO.4).

Effectiveness, proportionality and dissuasiveness of sanctions

516. Relevant legislative acts provide for sanctions, mostly fines, in cases of breaches of information requirements and other obligations by legal persons. The amount of fines varies depending on the type of legal entity and specific obligation or particular circumstances (see R.24). The competent authority for imposing sanctions differs based on the type of legal person and applicable legal obligations.

517. The evaluators were informed about 22 cases of possible breaches of information requirements by companies that were initiated in 2012-2016. Unreported changes of seats were suspected in 19 cases, but cases were discontinued, because the companies in question ceased operating and were subsequently removed from the relevant register. In the remaining 3 cases, companies were given warnings for breaching the time limit (15 days) for reporting changes in legal representatives and directors. No further details were provided on these cases or measures applied against other types of legal entities. The evaluation team could thus not conclude that sanctions applied against legal persons for breaching information requirements are sufficiently effective, proportionate and dissuasive. The lack of sanctions could also impact the overall effectiveness of existing mechanisms for ensuring that information kept in the registry is accurate and up-to-date.

518. The APMLFT contains sanctions for obliged entities in case of breaches of CDD requirements (see R.10 and R.24). Increased supervisory measures applied by BoS in recent years substantially improved the level of compliance among banks regarding obligations to identify and verify beneficial owners, however BoS has never imposed pecuniary sanctions due to the length of its proceedings (see also IO.3). BoS reported the following statistics on violations identified during on-site inspections and relevant measures applied:

Year	**Number of on-site inspections conducted**	**Number of on-site inspections where breaches regarding BO was detected**	**Supervisory measures**
2010	9	4	Letter with warnings (4)
2011	10	3	Order to eliminate violations (3)
2012	7	1	Order to eliminate violations (1)
2013	5	0	N/A
2014	6	1	Order to eliminate violations (1)
2015	6	0	N/A
Total:	**43**	**9**	**Letter (4), Order (5)**

Overall Conclusions on Immediate Outcome 5

519. Slovenia has a quite strong tradition of ensuring transparency in the basic ownership of legal persons, but there are some concerns about the effectiveness of existing mechanisms to ensure that the information kept in registers is accurate and up-to-date. In obtaining the beneficial ownership information, authorities mostly rely on banks that have substantially improved the implementation of CDD measures and are able to identify and verify ultimate beneficial owners to a considerable extent. Although no in-depth formal assessment of vulnerabilities of legal persons operating in the country has been conducted, the competent authorities appear to be generally aware of major risks. A number of safeguards and mechanisms do exist to help prevent the misuse of legal persons, although the evaluators are not convinced that these have proven to be sufficiently effective. Recently adopted additional measures are intended to reinforce the transparency of legal persons and arrangements, but their impact must be assessed over time.

520. **Overall, Slovenia has achieved a moderate level of effectiveness for Immediate Outcome 5.**

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

1. The authorities proactively seek and deliver international cooperation by using the applicable legal framework and instruments, secure information exchange channels and liaison networks. Although in the period under review comprehensive statistics on MLA have not been collected, several good examples of international cooperation have been produced demonstrating that Slovenia proactively seeks MLA, including in areas of increased of risk, and has achieved relevant results. Successful cases of international cooperation in relation to in-coming MLA requests have also been presented which have resulted in convictions and confiscation of property.

2. The OMLP and LEAs actively engage in international cooperation, including by proactively setting up Joint Investigative Teams with counterparts from other countries. They request assistance from foreign counterparts and provide timely and good quality assistance to competent authorities from other countries (both EU and non-EU).

3. Authorities provide and respond to foreign requests for cooperation in identifying and exchanging basic and beneficial ownership information of legal persons registered in Slovenia. However the weaknesses identified under IO.5 could potentially affect the authorities' ability to exchange beneficial ownership information in cases of legal persons established in Slovenia by foreign legal entities.

4. Although out-going MLA requests have been assessed as being sufficiently clear by global partners, Slovenia has experienced delays in receiving information on beneficial ownership of complex legal structures from foreign partners. The OMLP has also experienced difficulties in obtaining beneficial ownership information from some European FIUs. In the absence of such cooperation usual MLA methods are used making the process much longer and thus less efficient.

5. The OMLP has generally a good cooperation with its foreign counterparts, and as a matter of practice, it sends spontaneous information to its foreign counterparts. It has, however, experienced persisting difficulties in receiving information from a neighbouring counterpart on specific typologies which has hampered the effective elaboration/use of intelligence and the opening of ML investigations in relation to this typology.

6. The Bank of Slovenia has performed supervision of subsidiaries (located outside of the EU) of one Slovenian bank considered to be of high risk for ML, including through on-site inspections. It also

exchanges information with home supervisors on branches and subsidiaries of foreign financial institutions located in Slovenia, and within licensing procedures.

7. Slovenia has not presented any cases where international cooperation has resulted in repatriation or sharing of assets neither with EU or non-EU countries.

Recommended Actions

Slovenia should:

1. Ensure that statistics on MLA and extradition, including those made through direct contact, are collected and provide an indication of the types of crime which they relate to, as well as the outcome and the result of international cooperation.

2. Continue to seek actively foreign legal assistance and extradition in cases with a cross-border element, especially with regard to foreign predicate offences. This also applies to informal and spontaneous exchanges of information between domestic law enforcement and supervisory authorities and their foreign counterparts.

3. Continue and increase its efforts to resolve the communication problems with the FIU and LEAs from its neighbouring jurisdiction, which seriously hamper the investigation and pursuit of ML with foreign underlying predicate offences.

4. Fully explore and pursue possibilities for effective international cooperation as available also under the legal instruments outside of the EU (e.g. direct communication and joint investigation team as foreseen by international treaties).

521. The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The recommendations relevant for the assessment of effectiveness under this section are R.36-40.

Immediate Outcome 2 (International Cooperation)

522. International cooperation is an important component of Slovenia's AML/CFT regime given its geostrategic position and its status as a transit country for drug trafficking and other forms of organised crime, which exposes Slovenia to an increased ML/FT risk originating from outside its borders. Most ML-related cooperation is undertaken with neighbouring countries, both from the EU and with non EU States from former Yugoslavia. The statistics provided by the authorities demonstrate that a significant portion of notifications sent by the OMLP to LEAs/Prosecution authorities for further investigation had an international dimension. For instance in 2015, out of 190 notifications related to suspicion of ML sent by the OMLP to the police/prosecutor, 92 cases concerned funds and assets deriving from predicate offences committed abroad, in particular in neighbouring countries (48% of all ML cases). As regards the investigation phase, in the period under review, out of 273 criminal reports on ML filed by the police, 27 reports were related to predicate offences committed abroad (around 10% of all ML cases).

Providing and seeking constructive and timely MLA and extradition

523.Slovenia has in place a satisfactory legal framework to provide MLA and extradition (please see R. 37 and R. 39 of the TC Annex). This framework is formed by an extensive list of multilateral and bilateral treaties. Although the deficiencies in the criminalisation of the FT offence may limit Slovenia's ability to provide MLA/extradition in FT cases, the 4th round MER noted that in practice, the incomplete criminalisation of terrorist financing has not been an issue. In the period under review, the Ministry of Justice and judicial authorities have reported that they have not received any MLA requests related to FT. Dual criminality is a precondition for the execution of coercive measures outside of the EU framework, and for extradition to third countries (see R. 37 and 39).

524.Pursuant to a number of bilateral and multilateral treaties which Slovenia has entered into, the Ministry of Justice (MoJ) is the central authority which is responsible for receiving and sending MLA

and extradition requests, in accordance with the principles of efficiency and rapidity of procedure.[64] The OMLP is the authority which is responsible for receiving and sending MLA requests pursuant to the Council of Europe's 1990 and 2005 Conventions for Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism. As indicated in the TC annex (R. 37), the Ministry of Justice and the OMLP have an electronic case-management system in place to ensure the timely prioritisation and execution of requests.

525. The authorities have informed the assessment team that until the end of 2015 the Ministry of Justice did not have an information system capable of processing statistical data on in-coming and out-going MLA requests with a break-down of the requests received or sent by type of offence. According to the authorities, only general statistics on MLA were collected on a yearly basis. In-coming and out-going extradition requests, on the other hand, were recorded manually in a register which broke down the information by underlying criminal offence, country of cooperation and information on the outcome of the procedure. Since 1 January 2016, a new electronic data processing system has been set up allowing MLA and extradition data to be collected and broken down by the number of requests received or sent, the number of requests responded to, granted or refused, the underlying criminal offence and the timeliness of the response. The Ministry of Justice has advised that between 1 January and 16 November 2016, 13 MLA requests related to ML were recorded: 9 outgoing and 4 incoming. Of the incoming requests, 3 have been executed and 1 is pending. Of the outgoing requests, 5 are pending, 1 has been refused and 3 are executed.

526. The MoJ transmits a request to the competent Slovene or foreign authority within one or two days. Organised crime and ML are treated as high priority and dealt with within the same day. The average duration of MLA proceedings in Slovenia is between one to two months and depends on factors such as its urgency and complexity. For simple requests, the MoJ can obtain the requested information very quickly and transmit it to the requesting authorities.

527. As concerns in-coming extradition requests, the statistics provided indicate that up to 34 extradition requests were received per year since 2010 (in total 134 extradition requests from 2010 to 2016 out of which 9 were refused). These requests were responded to on average between 36 and 200 days. Grounds for refusal are, for in-coming requests, related to difficulties in finding the person (e.g. if he/she does not have any property or an address registered in Slovenia); for out-going requests, dual criminality issues and the statute of limitation. Extradition cases are transmitted as a priority and the related documents are sent to the competent judicial authorities on the same day they are received, or the day after. Between 2010 and 2016, a total of 89 extradition requests were sent to foreign counterparts (an average of 12 to 16 per year), three of them being related to ML. Seven of these requests were refused.

Table 20: **Extradition requests – incoming**

	Received	**Pending**	**Refused**	**Executed**	**Average time of execution (days)**
2010					
ML	**0**	**0**	**0**	**0**	**-**
Predicate offences	**11**	**0**	**0**	**11**	**90**
2011					

[64] Article 200 of the CPC foresees that the urgency in cases involving detention also applies mutatis mutandis to the extradition procedures.

ML	**1**	**0**	**0**	**1**	**36**
Predicate offences	**33**	**0**	**5**	**28**	**78**
2012					
ML	**0**	**0**	**0**	**0**	**-**
Predicate offences	**27**	**0**	**3**	**24**	**65**
2013					
ML	**0**	**0**	**0**	**0**	**-**
Predicate offences	**11**	**0**	**0**	**11**	**83**
2014					
ML	**1**	**0**	**0**	**1**	**200**
Predicate offences	**19**	**1**	**1**	**17**	**97**
2015					
ML	**0**	**0**	**0**	**0**	**-**
Predicate offences	**11**	**1**		**10**	**58**
2016 (up until mid-November)					
ML	**1**	**0**	**0**	**1**	**120**
Predicate offences	**19**	**8**	**0**	**11**	**48**

Table 21: **Extradition requests – outgoing requests**

	Sent	**Pending**	**Refused**	**Executed**	**Average time of execution (days)**
2010					
ML	**0**	**0**	**0**	**0**	**-**
Predicate offences	**12**	**1**	**0**	**11**	**-**
2011					
ML	**0**	**0**	**0**	**0**	**-**
Predicate offences	**16**	**0**	**2**	**14**	**-**
2012					
ML	**0**	**0**	**0**	**0**	**-**

Predicate offences	11	0	4	7	-
2013					
ML	0	0	0	0	-
Predicate offences	12	0	1	11	-
2014					
ML	0	0	0	0	-
Predicate offences	8	4	0	4	-
2015					
ML	1	1	0	0	-
Predicate offences	14	6	0	8	-
2016 (up until mid-November)					
ML	2	1	0	1	40
Predicate offences	13	8	0	5	56

528.The evaluation team notes that no detailed statistics were provided by the authorities on MLA between 2010 and 2015. The MoJ advised that over the past years, it has received and sent approximately 900 incoming and outgoing MLA requests per year of which the majority were related to criminal offences such as theft, illicit trafficking in narcotic drugs, fraud, counterfeiting and extortion. It estimates that it has transmitted approximately 15 requests related to ML per year. The evaluation team notes that it is difficult to quantify the number of in-coming and out-going MLA requests through direct cooperation given the absence of a case management system for direct communication between judicial authorities based on EU instruments. The authorities are of the opinion that the establishment of statistics on direct international cooperation would not be reasonable. Thus, it is not possible to determine with certainty the exact figures of MLA and extradition requests received or sent related to ML, FT and predicate offences nor the underlying predicate offences in the period under review. In the absence of this information, it is difficult to assess whether international cooperation efforts reflect areas of increased risk as far as crimes with a transnational element are concerned – these include drug trafficking, tax evasion but also foreign bribery and organised criminality. Nonetheless, the authorities have presented the evaluation team with several good examples of international cooperation demonstrating that they have proactively sought MLA from other States and have convicted defendants and/or seized and confiscated proceeds as a result. These case examples reflect several areas of increased risk (in relation to predicate crimes with transnational elements), including drug trafficking and organized crime. As for in-coming requests, a few successful cases of international cooperation have been presented which have resulted in convictions and confiscation of property (see below for an example).

529. As concerns the feedback received from the global network, there were not many examples of in-coming MLA requests to Slovenia – four were received by the central authorities and one was sent directly to a Court. While the request sent to the court was promptly satisfied, two jurisdictions indicated that their MLA request sent to the central authorities went unanswered. The third request was satisfied and the fourth was refused due to lack of dual criminality (according to the Slovene authorities it concerned a request for coercive measures of search and seizure). No specific feedback

was given with respect to incoming extradition requests. As concerns out-going MLA requests, the feedback received from the global AML/CFT network indicated that out of 26 out-going MLA requests, only one request was not sufficiently clear.

Box 15: Example of cooperation – Incoming request

The Federal Bureau of Investigation (FBI) while performing undercover operations on the Internet, discovered the sale of a high-performance virus and the transfer of the purchase price to a physical person in Slovenia via Western Union. An MLA request was sent by the USA to the Slovenian Police in order to carry out the search of the domicile of the suspect. The US authorities took part in the house search and in the collection of evidence. Once the suspect had been identified, the US authorities requested the suspect's extradition, which was refused. As a result, the Slovenian State Prosecutor's Office started to direct the pre-trial investigation and ordered the collection of evidence. This lasted several months and included both conventional MLA on the basis of the CPA, cooperation with US representatives, representative officers of Eurojust, and direct oral and written contacts with the FBI and the US federal prosecutor.

As a result of the investigation, Defendant A) was charged with "manufacturing of instruments intended for the commission of criminal offence" (instruments intended for the breaking or illegal entry into the information system), money laundering and aiding in the commission of an attack on information systems. Defendant B) and C) were charged with money laundering . Defendant A was sentenced to four years and ten months of detention and fined 3,000 Euro. The Court also ordered the confiscation of his apartment, computer equipment for an amount of 25,320.56 Euros and his personal vehicle. Defendant B was sentenced to a suspended sentence eight months and a term of suspension of two years. The convictions are final.

Box 16: Example of cooperation – Outgoing request

Slovenian Police obtained information on the transportation of illicit drugs (cocaine) while carrying out an undercover operation (an undercover operative transported 18,22 kilos of cocaine from Slovenia to the United Kingdom). The organization and the execution of the transportation of illicit drugs was carried out in cooperation between two Slovenian citizens, one person from the Netherlands with unknown citizenship and by three Albanian nationals living in London - the final destination of the transported drugs and the place in which the arrests were made.

The State Prosecutor's Office proposed to the Slovenian investigative judge to order an undercover measure of controlled delivery of the transportation of illicit drugs in Slovenia and to obtain investigative orders also from the courts of all the countries through which the cocaine would transit (Austria, Italy, Germany, France, Holland, Belgium and the United Kingdom). The two Slovenian citizens who were prosecuted in Slovenia were convicted and sanctioned with six years and six months of detention (defendant A) and five years and ten months (defendant B) for the organization of the transportation of illicit drugs. Confiscation of proceeds of crime was ordered only in relation to the purchase price. The remaining four defendants were prosecuted and convicted in the United Kingdom.

Box 17: Other examples of out-going MLA requests

One out-going MLA request concerned a criminal investigation on self-laundering (concealment and transfer of proceeds of crime) and the underlying predicate crime of accepting a bribe. In the context of this case an MLA request was sent to country A to obtain bank data and documents, request a hearing of the defendant and a witness and request the seizure of proceeds of crime; an MLA request was sent to country B to obtain bank data and bank documents and hear a witness; another request was sent to Country C to obtain bank data and documents; an MLA request was also sent to country D to hear a witness. Most of the requests were executed.

Another case example concerns a criminal investigation against several persons accused of money laundering and abuse of position or trust in business activity. The Slovenian court ordered the seizure of proceeds of crime for over 400.000 Euros and sent a request for seizure of assets to the State in which the defendants held their bank accounts. The competent prosecutor of the requested state informed Slovenian authorities that the proceeds of crime were seized for the whole duration of the criminal proceedings against the defendants.

530.The increased use of direct communication between judicial authorities of EU member states under the CCMMSEUA has resulted in a decrease in the amount of incoming and outgoing requests for MLA and extradition dealt with by central authorities. As concerns prosecution authorities in particular, each state prosecutor may receive or make requests related to international co-operation through direct contacts with foreign counterparts within the European Union.

531. Slovenian Prosecutors participate in and are also supported by Eurojust, which is of assistance in obtaining evidence and necessary information to decide whether to commence or continue criminal proceedings or in facilitating requests for MLA. There has been a rise in the number of requests for assistance from prosecutors through Eurojust during pre-trial procedures. In 2014, Slovenian competent authorities have requested to obtain operational assistance from other member states through Eurojust in 104 cases; in 2015 in 109 cases. ML was in second position among the criminal offences dealt with in these cases (17 cases), behind fraud, including business fraud and tax evasion (30 cases). The number of cases in which Slovenia has been requested to provide assistance via Eurojust was 41 in 2014 and 49 in 2015. The majority of these requests related to ML, fraud and drug trafficking.

532. Direct communication between judicial authorities for MLA is also allowed between non-EU member states, on the basis of treaties or if reciprocity applies. The authorities have advised however that it is quite rare to use direct communication between judicial authorities from non-EU countries. Mutual legal assistance with those countries mostly takes place through official channels, which are believed to be not very fast.

533.The current legal framework (see under R.38) allows cooperation and co-ordination with other countries on asset identification, seizure and confiscation. As noted above, the OMLP is the central authority for transmitting requests under the relevant Conventions for this cooperation. The OMLP has provided statistics on in-coming and out-going requests under Council of Europe Conventions CETS No. 141 and CETS No. 198 (see Table 22).

Table 22: **Requests based on CETS No. 141 and 198**

Year	**Out-going**	**In-coming**
2012	4	
2013	19	
2014	25	1
2015	29	
2016 (up until mid-November)	12	

534. The authorities note that the first requests sent under CETS No. 198 revealed the need to clarify how to make use of the Conventions' provisions in practice. After addressing practical questions at the national level, and further to the ratification of the Convention by an increased number of countries, there has been an increase in requests. The OMLP has continued to provide guidance to Slovenian courts on the use of the provisions and the details that need to be included in requests. With regard to outgoing requests, most requests under CETS 198 were made to EU member states.

When possible, the OMLP advises the courts to use EU mechanisms for direct communication instead.

Box 18: Freezing request

The District court of Ljubljana asked the OMLP in June 2015 to send a request to another State Party on the basis of CETS 198. The request concerned the freezing of proceeds of over 2 million Euros. The request was immediately forwarded to the competent foreign ministry, which provided feedback on the steps taken by the public prosecutors. All feedback received by the OMLP was forwarded to the District court of Ljubljana. After the initial request for freezing, two requests regarding the prolongation of the Court's freezing order were received by the OMLP and immediately forwarded to the competent foreign authority. The case is on-going.

535. As concerns the sharing of confiscated assets with other countries, while this is allowed with EU member States (and with non-EU countries under relevant treaties), the authorities did not provide any example of such cooperation in practice (see IO.8).

Seeking and providing other forms of international cooperation for AML/CTF purposes

Providing information

536. The OMLP provides information to foreign FIUs, both spontaneously and upon request, in a timely and effective manner. In response to requests received from foreign FIUs, the OMLP can access and provide administrative, law enforcement and financial information. In addition to providing financial information which is available and recorded in the OMLP database to the foreign FIU (STRs, CTRs and cross border transfers of cash exceeding 10.000 EUR), the OMLP may also forward information which it requests from obliged entities for the purpose of international cooperation (e.g. information on bank accounts and data on single transaction carried out in relation to a specific account opened by a customer). The OMLP's ability to cooperate is not subject to the indication of the predicate crime by the foreign FIU.

537. Responses to requests sent by foreign FIUs are provided on a timely basis, and in line with Egmont principles. Statistics show that, on average, requests were responded to within 18 days. Information is exchanged with foreign FIUs in a secure manner, mostly via the Egmont Secure Web (ESW) or FIU.NET.

Table 23: **OMLP Co-operation with other FIUs (EU and Non-EU)**

International co-operation	2010	2011	2012	2013	2014	2015	30.4.2016	Total
INCOMING REQUESTS								
Foreign requests received by the FIU*	**120**	**97**	**145**	**146**	**164**	**165**	**62**	**899**
Foreign requests executed by the FIU	99	86	141	146	164	165	62	863
Foreign requests refused by the FIU**	21	11	4	-	-	-	-	36
Spontaneous sharing of information received by the FIU	**5**	**6**	**2**	**4**	**13**	**15**	**12**	**57**
TOTAL (incoming requests and	**125**	**103**	**147**	**150**	**177**	**180**	**74**	**956**

information)								
Average number of days to respond to requests from foreign FIUs	**19,5**	**18,7**	**17,6**	**17,4**	**17,6**	**18,2**	**18,5**	**18,2 (average)**
Refusal grounds applied**	**8**	**7**	**4**	**-**	**-**	**-**	**-**	**19**
OUTGOING REQUESTS								
Requests sent by the FIU	**210**	**145**	**170**	**148**	**193**	**201**	**83**	**1.150**
Spontaneous sharing of information sent by the FIU	**1**	**-**	**3**	**12**	**21**	**53**	**61**	**151**
TOTAL(outgoing requests and information)	**211**	**145**	**173**	**160**	**214**	**254**	**144**	**1.301**

***This number includes all foreign requests, also those which were not recorded as STRs in OMLPs databases (the number of such requests was 47 in 2010, 76 in 2011, 60 in 2012, 74 in 2014, 70 in2014, 99 in 2015, 50 in 2016 (until 30.4.2016)**

****OMLP replied to all foreign requests, but to incomplete requests it provided only data from its own databases (STR, CTR, cross border transfers of cash) – regardless to the questions stated in the foreign requests. OMLP asked foreign FIUs to send the additional data on the case according to the EGMONT Group Best Practices for the Exchange of Information between the FIUs.**

538. From 2010 to April 2016, the OMLP received 899 requests from foreign FIUs. The number of incoming requests has been on the rise since 2011. Between 2010 and 2016, 36 requests were refused. If the OMLP considers that the request is incomplete, it invites the foreign FIU to send additional information related to the case. As indicated in the analysis of R. 40, the prioritisation of the requests received is made on a case-by-case basis and in accordance with the principles for information exchange provided under international agreements. No other guidelines or methodologies have been produced. The main trigger for prioritisation is the urgency level given by the requesting FIU or instructions provided from the Director of OMLP or the Head of the Analytical Unit.

539. After receiving a foreign request, the OMLP may either send a response to the foreign FIU without opening its own case (476 requests), or send the response and open its own case at the same time. If the suspicion described in the foreign request is related to a Slovenian natural or legal person, their business relationship, or any other contractual relationship established in Slovenia (e.g. bank account) the OMLP is likely to open a case in order to start its analysis. When a foreign FIU in its request specifically requires banking information, the OMLP must open a case in order to approach the relevant bank. Between 2010 and 2015, the OMLP opened 110 cases on the basis of foreign requests. In 96 of these cases there were sufficient grounds to believe that ML/FT had been committed and thus they were sent to the police/prosecutor or tax administration for further checks. The statistics show that, on the basis of foreign requests, the subsequent analysis by the OMLP confirmed the suspicion of ML or other criminal offences in 87% of cases. Out of the 96 cases in which an investigation was opened, four are at the prosecution stage while two cases are pending before the Court. The OMLP provides spontaneous feedback to foreign FIUs concerning the status of cases which were opened and analysed on the bases of their requests, notably whether the case was sent to the police/prosecutor for further investigation.

540. The OMLP has also provided spontaneous information to foreign FIUs in 151 instances. This practice has been on the rise in recent years; while in 2012 there were only 3 instances in which

information was spontaneously shared, in 2015 and 2016 these figures significantly increased (e.g. 61 requests registered by the end of April 2016).

541. Given that feedback is not provided to the OMLP by foreign FIUs in all cases, it is difficult to assess the number of investigations or prosecutions arising from co-operation between the OMLP and foreign FIUs. Feedback received from neighbouring countries shows that in a significant number of cases in which information was sought from and was received from the OMLP, the case was sent for further investigation to the police/prosecutor.

Seeking information

542. Between 2010 and April 2016, 1150 out-going requests were sent to foreign FIUs. The number of outgoing requests has been on the rise in the past years with 160 outgoing requests in 2013, 214 in 2014 and 254 in 2015. The number of outgoing requests is approximately 36% higher than the number of incoming requests. There have been 57 instances since 2010 in which spontaneous information has been received by a foreign FIU.

543. The authorities have informed the evaluation team that they have experienced some difficulties in receiving information from certain foreign counterparts, mostly related to delays in the provision of information. In particular, Slovenia has experienced difficulties in receiving information from a Country X FIU in relation to a specific typology. Slovenia is a ML destination country for funds from Country X, allegedly deriving from tax evasion and from proceeds of criminal organizations; use of corporate vehicles is also frequent practice. The typology is the following: a national from country X acting as a straw-man, opens a non-resident bank account at a bank office near the Slovenian-Country X border (including on behalf of a private legal person which s/he has established in Slovenia). Then the money is wired to this account and withdrawn in cash. In 2015 out of 190 written reports sent by the OMLP to the Police on ML suspicion, 60 (31%) were related to assets derived from predicate offences committed in Country X. Due to the difficulties experienced in obtaining information from the FIU of this jurisdiction, the OMLP no longer sends requests on these typologies to its counterpart. Instead, it sends the analysis of the activities it has undertaken and its findings with regard to these cases on a periodic basis. In return, however, the OMLP rarely receives from its counterpart information on the predicate crimes committed in Country X which could be used for investigation/prosecution purposes. The evaluation team was informed that the FIU from Country X sends the information received from the OMLP to LEAs of their jurisdiction, which, in turn, exchanges the data on the predicate offence with the Slovenian Police. However, since 2012 the Slovenian Police has filed only 19 criminal complains for ML with the underlying predicate offence committed in Country X. When comparing this data with the 60 reports sent only in one year, it is clear that for the majority of the STRs related to this typology, Slovenia does not receive feedback from its counterparts which would allow it to identify the predicate crime and provide sufficient information to LEAs to initiate an investigation. The lack of feedback, combined with the perception of high evidentiary threshold requirements in order to pursue autonomous money laundering cases (see IO.7), have hampered in practice the effective use of financial intelligence, the opening of investigations, as well as the prosecution of ML in connection with tax evasion and/or organised crime committed in the relevant jurisdiction (see IO.6).

544. The Slovenian FIU and Police have been proactive in trying to resolve the above-mentioned problems with its counterparts from Country X. A number of meetings have been organised, however no concrete results have so far been achieved.

Cooperation between Law Enforcement Authorities

545. Slovenian police regularly exchanges information at the operational and strategic level with its EU and non-EU counterparts either through Interpol/Europol channels or through informal meetings such as the Anti-Money Laundering Operational Network (AMON). Several bilateral and multilateral agreements and protocols have been signed for this purpose (more details can be found in R.40). Information exchanged between the Slovenian police and foreign LEAs can be used only for preliminary criminal proceedings. Although, as indicated in the TC annex under Criterion 40.7 the

Law on Duties and Powers of Police does not expressly provide for the protection of data received from foreign LEAs in the context of international cooperation (it only refers to information collected at the domestic level), in practice, this has not created any problem.

546. Statistics are kept by the police authorities on information exchanged through all of the operational channels (INTERPOL, Europol, SIS, internal mail, etc.).

Table 24: **Law enforcement agencies co-operation**

International co-operation	2010		2011		2012		2013		2014		2015		x.x.2016	
INCOMING REQUESTS	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**
Foreign requests received by LEAs related to ML	11	9	199	10	156	7	194	1	195	2	227	2	79	2
Foreign requests executed	11	9	199	10	156	7	194	1	195	2	227	2	79	2
Foreign requests refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TOTAL	**11**	**9**	**199**	**10**	**156**	**7**	**194**	**1**	**195**	**2**	**227**	**2**	**79**	**2**
Average time of execution (days)	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**	**NA**
OUTGOING REQUESTS	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**	**ML**	**FT**
Number of requests sent abroad by LEAs	22	0	101	0	72	0	68	1	92	1	115	2	34	0
Number of requests sent and executed	22	0	101	3	72	0	68	1	92	1	115	2	34	0
Number of requests sent and refused	-	-	-	-	-	-	-	-	-	-	-	-	-	-
TOTAL	**33**	**9**	**300**	**13**	**228**	**7**	**262**	**2**	**287**	**3**	**115**	**2**	**34**	**0**

547. Between 2010 and 2016, the Police received 1061 foreign requests for ML and 33 for FT; all of the requests were executed and replied to. In the same period the Slovenian Police sent 504 requests for cooperation to foreign counterparts for ML and four for FT, all of which were executed. The prioritisation of correspondence is done on a case-by-case basis – there are no additional guidelines to assist the authorities. In practice cases involving a deadline, the blocking of a transaction, an arrest or serious cases of violation of human rights are dealt as a priority and are labelled "urgent". The authorities indicated that the average time needed to respond to requests varied and depended on

the complexity of the matter, however all incoming requests are dealt with promptly and in a timely manner.

548. As indicated under Criterion 40.19 of the TC annex, Special Investigative Teams and Joint Investigative Teams may be formed under Slovenian legislation to facilitate cooperation between LEAs belonging to different jurisdictions. Between 2010 and 2016 Slovenia has proactively initiated one joint investigation team with the counterpart from another jurisdiction and has been involved in another joint investigation team set up by other countries. Both of the JITs facilitated cooperation in the investigation of money laundering and related predicate criminal offences.

Box 19: Set-up or involvement of the Slovenian Police in JITs:

A JIT involving Slovenia (the Specialised State Prosecutor's Office of the Republic of Slovenia) and Germany (Department of Public Prosecution Bochum) was set up on the initiative of Slovenia on 14 May 2014. Its purpose was to investigate and dismantle an organised crime network active in the area of illegal betting, specifically in relation to manipulated sporting events, in addition to the related offences of bribery, fraud including betraying, corruption and related money laundering. Defendant A and B were charged with bribery and defendant C with corruption. Defendant A was convicted as charged to a combined sentence of three years of imprisonment and a fine of 25,346 Euros. Defendant B was also sentenced to one year of imprisonment and to fine of 6,600 euros. The trial is on-going for defendant C.

Slovenia on 21 November 2014 joined a JIT set up by Finland, Romania and United Kingdom. Its purpose was to facilitate the investigations of offences committed by an organised criminal group in the above-mentioned countries, notably: offences committed on the Internet, including offences related to compromising websites, gaining unauthorized access to servers, stealing data, distributing and/or selling stolen data and money laundering. Eleven defendants were charged for various criminal offences: grand larceny; attack on information systems; use of a counterfeit bank, credit, or other card; and money laundering. Some of the defendants were sentenced to a prison term and a fine; others were given suspended sentences and for one defendant the trial is on-going.

Box 20: International cooperation case - POLICE:

In 2015-2016, Slovenian police investigated a case of ML and its predicate offence involving the fraudulent use of businesses' information systems. Malicious software was used to hack and access the information system of foreign companies registered abroad. In particular, through malicious software the suspects sent e-mails to companies' accounting departments using the director's e-mail account. The e-mails instructed the accounting departments of the respective company to transfer money into the bank account of a dummy company which the suspects had founded for criminal purposes. In order to register and found the dummy company and open the bank account the suspects also had provided false data (forged identity cards).

Once the money had been transferred by various legal entities to the bank account of the dummy company, the suspects further transferred through e-banking these sums to domestic and foreign bank accounts of other companies. In the course of the preliminary proceedings, the court found that the suspects had tried to launder 1.7 million EUR of illegal proceeds. In cooperation with the OMLP, 1.4 million euros were frozen and subsequently seized.

Given that the suspects had carried out money transfers abroad and had withdrawn money at ATMs and banks in various jurisdictions, many formal and informal meetings were held with foreign law enforcement authorities (Croatia, Bosnia and Herzegovina, Seychelles, Hong Kong, Latvia). Close cooperation was ensured with representatives of the Croatian law enforcement authorities and extensive operational information was exchanged with representatives of the Bosnian law enforcement authorities via INTERPOL. In addition, an MLA request was sent to obtain

data from law enforcement authorities from the Seychelles and Hong Kong.

Cooperation between Supervisory authorities

549. With regard to international cooperation between supervisors, the Bank of Slovenia has performed supervision of subsidiaries located abroad of one Slovenian bank, and based on the country's high risk profile with regard to corruption. Within this supervision, on-site inspections took place in two countries in cooperation with the host supervisors. As a general principle, the BS exchanges information with foreign counterparts that are home supervisors about relevant findings of inspections of subsidiaries and branches located in Slovenia. In two cases, the home supervisor then decided to come to Slovenia for an on-site inspection. BS advised the assessment team that its communication with foreign counterparts is mostly informal. The licensing department of the BS contacts foreign supervisory bodies when needed. The authorities provided an example of a case in which a license was refused based on information requested from a foreign counterpart supervisor.

Box 21: International cooperation in licensing

In 2011, company A submitted an application to BoS for authorization for the provision of payment services as a payment institution. In the process of examination of the application, the BoS noted some suspicious circumstances related to the acquiring of qualifying shares in company A of a seller (person X) who had close ties with the former director of another foreign-owned company (company B).

BoS contacted the National Bank of the foreign country for further information. It obtained information that company B was prohibited from the continuation of the provision of financial services and was removed from the official list of financial intermediaries in the foreign country. The grounds for these measures were criminal offenses and infringements in the field of money laundering, conducted by company B's management.

With regards to identified links between the applicant and person X, BoS requested the OMLP for their official position on the matter. The Office estimated that the authorization of the applicant to provide payment services would extremely increase exposure of the Slovenian financial system to attempts of money laundering.

On the basis of the findings during the examination process, BoS rejected the application of company A.

550. Despite having adequate legal powers to engage in international cooperation on AML/CFT issues with their foreign counterparts (see R.40), other supervisory authorities in the financial sector (Securities Market Agency and the Market Inspectorate) indicated that there had been no international cooperation for AML/CFT purposes. They maintained that such cooperation would be carried out through the OMLP. The Insurance Supervision Agency reported that it has sent 4 requests in 2015 to foreign counterparts specifically related to AML/CFT.

International exchange of basic and beneficial ownership information of legal persons and arrangements

551. The authorities provide and respond to international cooperation requests related to the identification and exchange of basic and beneficial ownership information of legal persons established in Slovenia. The feedback provided by the global network does not suggest particular concerns in this respect. However the weaknesses identified under IO.5 could potentially affect the authorities' ability to exchange beneficial ownership information in cases of legal persons established in Slovenia by foreign legal entities.

552. The authorities have experienced delays in receiving information on beneficial ownership of complex legal structures and on legal arrangements from their foreign counterparts. The OMLP has also experienced difficulties in obtaining beneficial ownership information from some European

FIUs. In the absence of cooperation provided directly, the MLA channel is used, making the process much longer and thus less efficient.

Overall Conclusions on Immediate Outcome 2

553. Slovenia has a strong legal framework for cooperation and provides constructive and timely assistance when requested by other countries. While the deficiencies in the criminalization of the FT offence may limit Slovenia's ability to provide MLA/extradition in this respect, in practice, no cases were presented indicating that the provision of MLA/extradition in relation to FT has been hampered. Although statistics on MLA and extradition have not been collected systematically, several good examples of international cooperation have been produced demonstrating that Slovenia proactively seeks MLA from other States in several areas of increased risk and has convicted defendants and/or seized and confiscated proceeds as a result. As for in-coming requests, successful cases of international cooperation have equally been presented which have resulted in convictions and confiscation of property. Furthermore, since 1 January 2016, a new electronic data processing system has been set up allowing collection of detailed data on MLA and extradition.

554. The OMLP and LEAs actively engage in international cooperation, including by proactively initiating the set-up of JITs. They request assistance from foreign counterparts and provide timely and good quality assistance to competent authorities from other countries (both EU and non-EU). The difficulties experienced in receiving information from a neighbouring FIU has hampered the effective elaboration/use of intelligence and the opening of ML investigations in relation to this typology. The authorities provide and respond to international cooperation requests related to the identification and exchange of basic and beneficial ownership information of legal persons established in Slovenia, however the weaknesses identified under IO.5 could potentially affect the authorities' ability to exchange beneficial ownership information in cases of legal persons established in Slovenia by foreign legal entities.

555. **Slovenia has achieved a substantial level of effectiveness for Immediate Outcome 2.**

TECHNICAL COMPLIANCE ANNEX

1. This annex provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerological order. It does not include descriptive text on the country situation or risks, and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.
2. Where both the FATF requirements and national laws or regulations remain the same, this report refers to analysis conducted as part of the previous Mutual Evaluation in 2010. This report is available from: http://www.coe.int/t/dghl/monitoring/moneyval/Countries/Slovenia_en.asp

Recommendation 1 - Assessing Risks and applying a Risk-Based Approach

3. At the time of the fourth MER, there was no requirement for assessment of ML/FT risks for the country or other risk-related requirements set out in R.1.

4. *Criterion 1.1* - Slovenia has conducted its first NRA in 2015 using the World Bank methodology. The NRA includes assessment of ML threats, national vulnerabilities and sectorial vulnerabilities. However it did not include a comprehensive assessment of FT risks, and authorities have not explored certain relevant factors in order to properly understand the ML/FT risks. The assessment of ML/FT risks in Slovenia has not been limited to the NRA project, but has also taken place within strategic analyses of the OMLP and within the context of multi-agency working groups against economic crime and terrorism. More information can be found in IO.1.

5. *Criterion 1.2* - The Slovenian Government appointed a temporary Interdepartmental Group for Execution of the NRA for ML and FT with the following duties: performing of NRA; preparation of the

report on ML/FT risks; preparation of the action plan on the basis of the findings of NRA; performing of other analyses in the field of ML/FT where coordination and cooperation between different institutions is needed and a report on analysis and proposed actions should be prepared. The Group consists of members from different institutions, with the coordination role vested in the OMLP. Art. 8 APMLFT provides for the establishment of a permanent interdepartmental working group responsible for ML/FT NRAs. At the time of the on-site visit, this group was not yet installed due to the very recent entry into force of the law.

6. *Criterion 1.3* - The first NRA was finalised in 2015. The statistical data related mostly to the 2010-2013 period. In November 2016, the authorities updated the first NRA report with data of the years 2014 - 2015 in order to proceed with the action plan (see further under 1.5). The ML/FT NRA shall be updated at least every four years (Art. 8 (1) APMLFT) – authorities advised that it can thus be updated on a timelier basis should new and emerging risks give reason for that. A few specific analyses have been planned for 2016-2017 to follow up on vulnerabilities in the legal framework identified in the NRA, of which one (on asset management, see IO.8) was finalised before the on-site visit.

7. *Criterion 1.4* - The Slovenian Government received the finalised first NRA report (in October 2015) and its updated version (in November 2016). The representatives of the stakeholders involved in the NRA process also received the final report. By the time of the on-site visit, only a summary of the results of the first NRA has been published on the OMLP's website[65]. No further outreach activities were conducted to inform the private sector of the NRA results, with the exception of the banking and securities sector.

8. *Criterion 1.5* - Slovenian authorities have elaborated several national policies and platforms which have shown ML/FT risk-sensitive features even before the elaboration of the first NRA (see IO.1). Slovenia has developed an Action Plan based on the updated NRA, which was received by the Slovenian Government only during the on-site visit. The Action Plan appears to be rather general and some of the prescribed mitigation activities can be interpreted ambiguously. It does not include CFT specific measures. Authorities' priorities do not yet take into consideration the risks identified in NRA.

9. Art. 9(2) APMLFT stipulates that findings of the NRA shall be used to improve the national AML/CFT regime and appoints the OMLP as the body responsible for directing and harmonising these actions. Furthermore, Art. 9(4) states that the Government shall determine the sectors/activities of lower or greater risk by governmental Regulation. By the time of the on-site visit, the Government had not yet issued such regulation. Having regard to the foregoing it can be concluded that Slovenia does not fully apply risk-based approach to allocate resources and implement measures to prevent or mitigate ML/FT.

10. *Criterion 1.6* - Slovenia allows specific complete or partial exemptions from application of AML/CFT measures for certain FIs and DNFBPs (Art. 5, 6 and 22 APMLFT) in line with the FATF standards: proven low risk as apparent from an assessment; limited and justified circumstances; for a particular type of institution or activity, financial activity (other than the transferring of money or value) is carried out by natural or legal person on an occasional or very limited basis (having regard to quantitative and absolute criteria). However these exceptions appear to be mostly based on presumption, rather than on proven low risk of ML/FT. The NRA has identified some of these entities/activities as low risk (e.g. electronic money, financial leasing, granting credit or loans, including consumer credit, mortgage credit, factoring, and the financing of commercial transactions, including forfeiture) but the NRA's limited analysis makes these results questionable.

11. *Criterion 1.7* - Enhanced measures were already in place before conducting the NRA, which have been maintained in the new APMLFT. Enhanced CDD should be applied in cases where the obliged entity assesses that there is a high risk of ML/FT due to the nature of the business relationship, form

[65] NRA was published in full in January 2017 on the OMLP website, http://www.uppd.gov.si/en/media_room/news/article/5/92/

or manner of executing the transaction, business profile of the customer, or other circumstances relating to the customer (Art. 14(2) APMLFT). These requirements are in line with the risk-based approach. Art. 59 APMLFT further prescribes enhanced CDD in cases of correspondent banking relations with third (non-EU/EEA) countries, PEPs, and cases when a customer was not physically present when his identity was determined and verified within CDD. The authorities have not provided evidence to the evaluation team indicating that these situations have been assessed as high risk and that consideration has been given to introduce enhanced measures for any other potential risky sectors or activities. The existing measures were not evaluated within the NRA or against the results of the NRA. The APMLFT foresees that the NRA's findings are to be used to define by governmental regulation sectors or activities where stricter CDD and other measures must apply (Art. 9 and 59). No such regulation had been issued by the time of the on-site visit and it did not become clear whether it has been considered.

12. Criterion 1.8 - If an obliged person assesses that a customer, business relationship, transaction, product, service, distribution channel, state or geographical area presents little ML/FT risk, it may use simplified CDD (Art. 14(1) APMLFT), which is in line with the risk-based approach. Simplified CDD measures are provided for in Art. 57-58 APMLFT (see R.10, R.22). Art. 57 in combination with Art. 9 (2) APMLFT stipulates that the results of the NRA *may* be taken into account when making this decision. Art. 9 APMLFT foresees that the NRA's results are to be used to define by governmental regulation sectors or activities of little risk. This had not happened by the time of the on-site visit and it did not become clear whether it has been considered.

13. *Criterion 1.9* - Art. 139 APMLFT lists the bodies which exercise supervision over implementation of the provisions of the Act, including the RBA obligations for FIs and DNFBPs as described under criteria 1.10-1.12.

14. *Criterion 1.10* - Obliged entities are required to assess ML/FT risks related to their customers, business relationships, transactions, products, services or distribution channels, taking into account geographical risk, in accordance with guidelines issued by the competent supervisor (Art. 13 APMLFT). The (procedure for the) risk analysis must reflect the specific features of the entity and its operations. The assessment must be documented and updated at least every two years. Findings shall be available to the competent supervisors on demand. Risk assessment must be performed *before* the introduction of a change in internal policies and measures must be adopted to reduce identified ML/FT risks.

15. *Criterion 1.11* - Obliged entities must ensure regular internal control over the performance of tasks for detecting and preventing ML/FT (Art. 81 APMLFT). According to Art. 82, the Minister of Finance will prescribe the detailed rules on compliance officer, method of performing internal control, retention and protection of data, managing of evidences and professional training of the employees of obliged entities according to APMLFT. These rules had not been issued yet at the time of the on-site visit. A special Rule issued by OMLP and BoS under the old APMLFT provides some more detail regarding internal control. The Rule contains no requirement for approval of internal controls by senior management. Obliged entities must apply enhanced CDD in identified high risk cases (Art. 14(2) APMLFT).

16. *Criterion 1.12* - Under the APMLFT, simplified CDD is possible in specified cases. It shall not be allowed if reasons exist to suspect ML or FT in relation to a customer, transaction, property or assets (Art. 57(7)).

Weighting and Conclusion

17. Slovenia has conducted its first NRA in 2015 and has updated the assessment in 2016, but authorities have not explored certain relevant factors in order to properly understand the ML/FT risks. The rather general Action Plan has only recently been adopted and it cannot be concluded that Slovenia applies a risk-based approach to allocating resources and implementing measures to mitigate ML/FT. Other concerns relate to outreach on risks and consistency of exemptions, enhanced and simplified measures with the risk assessment. **Slovenia is partially compliant (PC) with R.1**.

Recommendation 2 - National Cooperation and Coordination

18. In its fourth MER, Slovenia was rated compliant with the requirements of the former R.31. The report concluded that overall cooperation and co-ordination appeared to be an important part of the system and was performed on a state, inter-ministerial, expert and operational level.

19. *Criterion 2.1* - Art. 8 and 9 APMLFT define in detail the NRA process and the responsibilities of the Inter-agency working group which is in charge of preparing the NRA report and its Action Plan. As indicated earlier, Slovenia has completed its NRA and has developed an AML/CFT Action Plan which is informed by the findings of the NRA. However, the NRA does not include a comprehensive assessment of FT risks.

20. Certain elements of AML/CFT prevention, coordination and cooperation are also included in some strategic documents such as the "National Security Strategy of the Republic of Slovenia" (adopted in 2010); "Resolution on National Program of preventing and fighting against Crime 2012 - 2016" (adopted in 2012); and the "Strategy of Managing Economic Crime in the Republic of Slovenia" (adopted in 2012). These documents also provide a division of responsibilities among competent authorities in tackling economic and organised crime, corruption, seizure and confiscation of crime proceeds. The OMLP has adopted its latest AML/CFT Strategy for 2016-2018.

21. *Criterion 2.2* - According to Art. 29 of the State Administration Act, the Ministry of Finance carries out tasks related to area of AML/CFT. The list of tasks is however not specified. Furthermore, Art. 21 of this Act stipulates that a *"body within ministry"* may be set up for purposes of efficiency and expertise, or if there is a need, for higher degree of autonomy in carrying out these tasks. On that basis the Government issued a "Decree on Bodies Within Ministries" (Official Gazette No. 35/15 of 22 May 2015 - with amendments) which, in its Article 5 states that the OMLP is a constitutive body of the Ministry of Finance assigned to AML/CFT tasks. The specific tasks of the OMLP are stipulated by the new APMLFT. In line with Article 87 APMLFT, the OMLP performs AML/CFT tasks and any other tasks which are regulated by this Act. In addition, specific duties related to the ML/FT prevention are determined in Art. 141 APMLFT, authorising the OMLP to propose to the competent authorities changes and amendments to regulations concerning the prevention and detection of money laundering and terrorist financing. Art. 8 (3) APMLFT, designates OMLP as a key institution which 'directs and coordinates the work and tasks of the permanent inter-ministerial working group established to carry out NRA'.

22. *Criterion 2.3* - In its Art. 7, the APMLFT requires the OMLP, the relevant supervisory bodies and other authorities competent to detect and prevent ML and FT to work together in order to harmonise and implement policies and activities. In order to achieve this goal, they may sign agreements on mutual cooperation and establish inter-ministerial working groups with the aim to attain both operational and policy level goals. In addition, strengthening co-operation and co-ordination among domestic authorities (including in the field of AML/CFT) is one of the goals of the "Resolution on National Program of preventing and fighting against Crime 2012-2016". The Resolution defines activities, which have to be performed by state authorities, independently or in cooperation with other bodies.

23. As concerns the coordination and cooperation of relevant authorities at the operational level, the Police and the Financial Administration of the Republic of Slovenia co-operate very closely with the OMLP. Special agreements on co-operation among these authorities have been entered into. In addition, the Criminal Procedure Code (Art. 160a and 160b) regulates the establishing and functioning of special investigative teams under the prosecutors' guidance. These teams are, *inter alia,* responsible for AML/CFT investigations. Furthermore, under the 2003 "Government Regulation on internal organisation, systematization, employment places and names in public and judicial bodies", a Permanent Coordination Group for Prevention, Detection and Prosecution of Money Laundering and Terrorist Financing was set up in 2012. The Group discusses problems arising in the field of prevention, detection of money laundering and terrorist financing. Its main responsibility is, inter alia, to exchange experiences and discuss legal issues arising from Slovenian legislation in relation to the prevention, supervision, detection and prosecution of money laundering and terrorist

financing; and compare Slovenian legislation and court practice with those of other countries. The group holds regular meetings, prepares and adopts its action plan and reports on activities of its members.

24. As concerns coordination and cooperation at a policy level, Art. 8(2) APMLFT provides that the Government shall establish a Permanent Inter-Departmental Working Group (chaired by the OMLP) responsible for carrying out ML/FT NRA and an action plan for mitigating the identified ML/FT risks. The Group also carries out any other analysis in the ML/FT field which requires co-operation and co-ordination among different institutions, and prepares reports on that analysis.

25. *Criterion 2.4* - A Permanent Coordination Group for Restrictive Measures was established in accordance with Article 1 of the Act on Establishing a Permanent Coordination Group for Restrictive Measures. The Group is in charge of monitoring and coordinating the implementation of restrictive measures. Moreover, the Group may establish ad hoc expert subgroups in order to perform specific tasks.

26. The Group is chaired by a representative of the MFA and includes members from the MoF, MoJ, Ministry of Economic Development and Technology, Ministry of Infrastructure, Ministry of Education, Science and Sport, MoI, Ministry of Defence, Ministry of Health, BoS, FARS, SISA, Slovenian Nuclear Safety Administration, Chemicals Office of the Republic of Slovenia, and OMLP. Members are appointed and dismissed by a decision of the Government of the Republic of Slovenia at the proposal of the Minister of Foreign Affairs.

27. The Group holds regular meetings, at least once a year and, if necessary, it may convene extraordinary meetings. The Act, however, makes no specific reference to proliferation issues. Nevertheless, the evaluation team is of the opinion that this mechanism is sufficient to answer the requirements of the criterion.

Weighting and Conclusion

28. Slovenia meets two of the criteria of recommendation 2. The AML Action Plan serves as the country's AML/CFT policy and is informed by the findings of the NRA, which, however, does not include a comprehensive assessment of FT risks. While a Permanent Coordination Group for Restrictive Measures has been set-up, the Act which establishes it, makes no specific reference to proliferation issues. **Slovenia is largely compliant (LC) with R.2.**

Recommendation 3 - Money laundering offence

29. Slovenia was rated partially compliant in the 4th round MER with regard to former R.1. As far as technical compliance is concerned, this rating was based on the fact that not all categories of offences were fully covered as predicate offences due to gaps in the FT offence.

30. *Criterion 3.1* - ML is criminalized under Art. 245 (1) CC and is also defined under Art. 2 APMLFT. The provision of the CC has not been amended since the last MER, which concluded that all the elements of Art. 3 (1)(b)(c) of the Vienna Convention and Article 6 (1) of the Palermo Convention were covered. Nevertheless, in the evaluation team's view acquisition and possession are not fully covered by the words 'accept' and 'store' used in the CC, although the authorities differ. Furthermore, information received during and after the on-site visit, indicates that the list of laundering acts under Art. 245(1) CC should be read as requiring the purpose of concealment. The Vienna and Palermo Conventions requires the criminalisation of simple acquisition, possession and use of illegal proceeds.

31. Indeed, relevant guidelines provide that the 'aim to conceal' is a necessary element which needs to be specified in disclosures from OMLP to Police or Police to the Prosecutor (see IO.6).

Furthermore, a 2015 judgment from the Supreme Court found that the 'aim to conceal' is a necessary element of the ML offence, at least in cases of self-laundering (see IO.7).[66]

32. Art. 217 CC criminalises whoever "*purchases, takes as a pledge or otherwise acquires, conceals or disposes*[67] *movable or immovable property which s/he knows to have been gained unlawfully*". This provision, as clarified by the authorities applies to third parties (it is not applicable to perpetrators of the underlying proceeds-generating offence). In the evaluation team's view, it covers acquisition of property knowing that it is proceeds of crime and does not cover "possession"[68] and "use" as per Art. 3 (1)(c) of the Vienna Convention. Therefore, a joint reading of Art. 245(1) and 217 of the CC implies that Slovenia is in line with Art. 3(1) of the Vienna Convention, with the exception of Art. 3 (1)(c) as it does not criminalise the act of ML in the form of simple possession and use of property.

33. Also, it should be noted that sanctions for Art. 217 are lower than for Art. 245 (see criterion 3.9), which also impacts on the types of ancillary offences that are applicable (see criterion 3.11)

34. *Criterion 3.2 and 3.3* - Art. 245 CC provides for an all-crime approach. The 4th round MER found that all designated categories of predicate offences are covered by the Slovenian legislation; there have been no major changes in this respect. Smuggling in relation to customs and excise duties and taxes and tax crimes related to direct and indirect taxes, which were introduced as predicate offences by the 2012 FATF Recommendations, are covered by Art. 249 – 250 CC. The concerns indicated in the previous MER with regard to the predicate offence of FT remains the same (see R.5). Thus all predicate offence categories but one are adequately covered.

35. *Criterion 3.4* - The wording "money or property" used in Art. 245 appears broad enough to cover all types of property, since there are no specifications. This interpretation was confirmed through discussions with practitioners on-site and through case law provided. The competent authorities further expressed their strong opinion that the ML offence can be extended to indirect proceeds, although no case examples or case law were provided to support this view.

36. *Criterion 3.5* - Pursuant to the wording of the law, it does not appear necessary that a person be convicted of a predicate offence when proving that property is the proceeds of crime. The authorities have provided two Supreme Court decisions confirming this view (No. I Ips 308/2009 from 16 September 2010; No. I Ips 75110/2010 from 10 July 2014).

37. *Criterion 3.6* - As concluded in the previous MERs, general provisions of the CC provide for application of the CC to Slovenian citizens committing offences outside of Slovenia and any person conducting offences outside of Slovenia under the condition of dual criminality (Art. 12, 13 (1) and (2), 14(3)). Combined with the all-crimes approach that Slovenia uses for predicate offences, it can be concluded that predicate offences for ML extend to conduct that occurred in another country as envisaged by the standard. The condition of dual criminality can be circumvented if a person commits a criminal offence abroad which, under relevant international agreement(s) or general legal rules recognised by the international community, is recognized as a criminal act and must be subject to prosecution regardless of the location where it was committed (Art. 13 (3)). The Minister of Justice has to give permission for the prosecution of the latter kind of cases (Ar. 14 (7)).

38. *Criterion 3.7* - Self-laundering is provided for in general terms and criminalised under Art. 245 (2) CC. However, from a joint reading of Art. 245(1), 245(2) and 217 (which does not apply in cases of self-laundering), it must be concluded that self-laundering in relation to simple acquisition,

---

[66] It must be recalled that, in Slovene legal system, judgments of the Supreme Court take place in individual cases. Although lower courts are not legally bound to follow the interpretations of the Supreme Court, the jurisprudence provides important guidance to the prosecution and judiciary services,

[67] Authorities have advised that 'to dispose of' must be understood in the sense of disseminating or putting into circulation.

[68] The authorities are of the opinion that possession would also be covered through this article given that acquisition is the act of gaining possession. However, the evaluation team maintains that possession can be exercised without having acquired property.

possession or use of proceeds of crime is not covered[69] . The "ne bis in idem" principle of the Slovenian Constitution (Art. 31) can justify the absence of criminalisation of self-laundering under these circumstances. Indeed, the 2015 Supreme Court judgment indicated that if the suspected perpetrator of ML is also prosecuted for the underlying predicate offence, it is necessary to prove subsequent activity or aim to conceal the proceeds; otherwise there cannot be two indictments for the same acts.

39. *Criterion 3.8* - The law does not expressly state that the intention and knowledge in the ML offence can be inferred from objective factual circumstances. In general, judges rely on the principle of free evaluation of evidence (Art. 18 CPC), which would enable them to make such inference. This was confirmed in the 2010 and 2014 Supreme Court decisions mentioned under 3.5, and through discussions with the judiciary on-site. However, in practice there still appears to be a strong reluctance to draw inferences from facts and circumstances, as was the case at the time of the 4th round MER (see under IO.7).

40. *Criterion 3.9* - The applicable sanction for ML (Art. 245 CC) is imprisonment of up to five years. For high value ML (involving money or property of over 50,000 EUR, see Art. 99 CC), it is up to eight years imprisonment and a fine, and when committed in a criminal association, the penalty is raised to one up to ten years and a fine. Negligent ML is punished with up to two years imprisonment. Within these ranges, the judge has discretion to determine the sentence based on proportionality considerations: the court shall consider all mitigating and aggravating circumstances, including degree of criminal culpability and motives for the offence (Art. 49 CC). Mandatory confiscation is also provided for in cases of ML (see R.4). Having regard to sanctions for other economic offences, these sanctions appear proportionate and dissuasive.

41. The available sanction for acquisition of proceeds (Art. 217 CC) when committed with knowledge is up to two years imprisonment and up to one year when committed with negligence. The penalty is raised to up to three years in case of high value of proceeds and to at least five years when committed in a criminal association.

42. *Criterion 3.10* - Under Art. 42 CC, legal entities can be held criminally liable for offences as statutorily determined. According to the Liability of Legal Persons for Criminal Offences Act (LLPA), legal persons may be held liable for ML offence. The liability of a legal person does not preclude the criminal liability of natural persons or responsible persons for the committed criminal offence (Art. 5 (2) LLPA). There is a range of sanctions which may be applied to legal persons (such as fine, confiscation, winding-up; Art. 12 LLPA). The criteria for application of punishments are provided for in Art. 26 LLPA and appear proportionate and dissuasive in the case of ML.

43. *Criterion 3.11* - There is a sufficient range of ancillary offences to the ML offence under the CC: Attempt (Art. 34); Solicitation (Art. 37); Criminal support, including counselling or instructing the perpetrator (Art. 38); Solicitation or support of a criminal attempt (Art. 39); Accomplice (Art. 20) in combination with Limits of incrimination of Accomplices (Art. 40); Criminal Association (Art. 294) and Criminal Conspiracy (Art. 295). Criminal conspiracy applies only when there is an agreement to commit an offence for which a punishment exceeds five years imprisonment, thus, it does not apply to basic ML. For acquisition of criminal proceeds under Article 217 CC without any aggravating circumstances, attempt or support of an attempt is not criminalised and solicitation is criminalised only when the incited act is really committed.

Weighting and Conclusion

44. Slovenian legislation is in line with Article 3(1) of the Vienna Convention, with the exception of Art. 3 (1)(c) as it does not criminalise the act of ML in the form of simple possession and use of property. All categories of offences with the exception of one are fully covered due to gaps in the FT

[69] As indicated under 3.1, acquisition and possession of proceeds are not covered under the ML offence and use is covered but only if there is the purpose to conceal. Article 217 does not apply to self-laundering.

offence. There are some minor deficiencies in relation to the scope of application of certain ancillary offences. Nonetheless, these deficiencies are deemed minor. **Slovenia is LC with R.3.**

Recommendation 4 - Confiscation and provisional measures

45. In the 2010 MER, Slovenia was rated partially compliant in relation to confiscation and provisional measures under R.3 of the then FATF Recommendations, based on effectiveness concerns. No technical deficiencies were identified. The standard now includes new requirements.

46. *Criterion 4.1* - The CC and CPC provide for the confiscation of the following:

A. **Property laundered.** Confiscation of money and property laundered by persons convicted for ML is mandatory, whether held by the perpetrator or a third party (Art. 245(6) CC). Objects which pursuant to criminal law may or must be confiscated shall be confiscated even when criminal proceedings do not end in a guilty verdict if there is a danger that they might be used for a criminal offence or where so required by the interests of public safety or by moral considerations (Art. 498 CPC). The court shall also impose confiscation of laundered property if there is no conviction for ML but if "those elements of criminal offences referred to in Article 245 of the Criminal Code [the ML offence] which indicate that money or property originate from criminal offences are proven" (Art. 498a CPC).

B. **Proceeds of (including benefits derived from such proceeds) or instrumentalities used/intended for use in ML or predicate offences**. According to Art. 74(1) CC, nobody shall retain the property gained through or owing to the committing of a criminal offence. Art. 75(1) CC provides for the mandatory confiscation of money, valuables and any other property benefit gained through or owing to the committing of a criminal offence, from the perpetrator or recipient. The CC does not provide for a definition of a term "property benefit". Supreme Court judgments have confirmed that the term is sufficiently broad to encompass benefits *derived from* proceeds of ML or predicate offences (Judgements No. I Ips 438/2006 dated 19 April 2007, No. I Ips 46801/2011 dated 22 January 2015). Instrumentalities (objects used or intended to be used or gained through the committing of a criminal offence) may be confiscated from the perpetrator. If instrumentalities do not belong to the perpetrator they may also be confiscated from third parties if required for reasons of general security or morality and if the rights of other persons to claim damages from the perpetrator are not thereby affected (Art. 73 CC).

C. **Property which is proceeds or used in/intended or allocated for use in the financing of terrorism, terrorist acts or organisations.** Art. 109(4) CC (FT offence) provides for mandatory confiscation of money or property provided or collected in order to partly or wholly finance the committing of a list of terrorist offences. Proceeds of terrorism, FT or terrorist organisations would qualify as property gained through or owing to the committing of a criminal offence which cannot be retained and would be confiscated (Art. 74 – 75 CC). Art. 498 CPC (see under A above) applies to the FT offence as well. Due to the technical deficiencies in the FT offence (see R.5), confiscation of property provided or collected is not available in the case of financing all terrorist offences as defined under the FT Convention or in the case of financing individual terrorists or terrorist organisation if the intention of the financier for the collection or provision of the funds was not directed at the committing of terrorist offences.

D. **Property of corresponding value.** If confiscation of property benefit gained through or owing to the committing of a criminal offence cannot be carried out, property equivalent to the property benefit shall be confiscated pursuant to Art. 75(1) CC. Furthermore, when the property benefit or property equivalent to the property benefit cannot be confiscated from the perpetrator or other recipient, the perpetrator shall be obliged to pay a sum of money equivalent to this property benefit (Art. 75(2) CC).

47. As an additional tool, Slovenia in 2011 introduced the Forfeiture of Assets of Illegal Origin Act (FAIOA), which provides a legal ground for civil asset forfeiture. Civil proceedings for the forfeiture of assets of illegal origin shall commence by a lawsuit brought against the owner as defendant by a state prosecutor of the Specialised State Prosecutor's Office as plaintiff.

48. *Criterion 4.2* - Proceeds gained through or by reason of the commission of a criminal offence shall be determined in criminal proceedings *ex officio* (Art. 499 CPC). The court and other agencies conducting the proceedings are bound to gather evidence and inquire into circumstances material to the determination of proceeds. If the injured party has filed an indemnification claim, the proceeds to be confiscated shall only be determined for that part which exceeds the claim. Chapters 15 and 16 CPC set out the powers for the police in the pre-trial and trial procedures to collect all information that may be useful for the successful conducting of criminal proceedings, including inspections of premises and documentation of enterprises and other legal entities. Art. 160a CPC prescribes the guiding role of the public prosecutor in this process and the possibility to establish a specialised investigation team involving other authorities (see further under R.31).

49. FAIOA provides legal grounds and powers for conducting financial investigations to gather the evidence and information required for civil asset forfeiture, independent from criminal prosecution. They shall be carried out when suspicion arises in pre-trial or trial proceedings that a person has assets of illegal origin in his possession with a total value exceeding EUR 50,000.

50. Since the provisions of the CPC are directed to proceeds gained through or by reason of the commission of a criminal offence and the provisions of FAIOA to assets of illegal origin, it may be concluded that there are no special legal provisions aiming to identify, trace and evaluate property subject to confiscation in cases of instrumentalities used or intended for use in ML or predicate offences or for property from legitimate sources intended or allocated for FT. The authorities consider that provisions of the CPC determining special investigative powers and techniques can nevertheless be used also in such circumstances to gather evidence.

51. Provisional measures for securing of criminal proceeds are available both in the trial and pre-trial procedure, against the accused or suspect, the recipient of the proceeds or another person to whom they were transferred provided they can be confiscated pursuant to the CC (Art. 502 CPC). The judge's ruling on the securing is served on the person simultaneously with its enforcement or after it without undue delay, whereupon the person has the possibility to get acquainted with the files of the case and raise objections with the right to be heard (Art. 502.a CPC). It thus follows that the initial application for provisional measures can be made *ex parte* and without prior notice.

52. It appears that the CPC does not regulate provisional measures concerning instrumentalities used for committing a criminal offence, which may impede authorities to carry out provisional measures for property laundered in autonomous ML and for legally obtained funds for FT. The authorities consider that the possibility for confiscation of objects upon court order which may represent evidence in criminal proceedings remedies this gap (Art. 220 CPC). Police officers can seize such objects even before the court issues an order when needed for detection and preservation of traces of crime or objects of value as evidence. Art. 20-25 FAIOA set out provisional measures for temporary freezing and forfeiture in civil proceedings.

53. A broad range of measures enable authorities to take steps that will prevent or void actions that prejudice the ability to freeze, seize or recover property subject to confiscation (Art. 75 (3)-(4), 77b and 77c CC). This includes a reverse burden of proof for close relatives when property has been transferred to them to avoid confiscation, in which case the property shall be confiscated unless they can demonstrate that they paid its actual value. Art. 6 and 27 FAIOA provide for a presumption of gratuitous transfer of assets if such assets have been transferred to closely related parties or immediate family members and reversed burden of proof in such cases.

54. *Criterion 4.3* –It can be concluded from the wording of the law that the rights of *bona fide* third parties are protected (Art. 500, 502.a, 504 CPC in combination with Art. 75 and 77 CC; Art. 73 and 76 CC; Art. 30 (1)-(2) FAIOA).

55. *Criterion 4.4* – Slovenia does not have a central asset management institution. Both for proceedings under the CPC and under FAIAO, the court decides on the competent authority for storage and management according to the nature of the assets (Art. 506.a CPC; Art. 24 (3) and 37 FAIOA). . For example, the competent authority for securities is the Slovenian Sovereign Holding; and

for movable property the Financial Administration. In both regimes, the court may order that property may be sold, destroyed or donated for the public benefit in case of disproportionate costs of storage or decreasing value. Mechanisms of managing and disposing of frozen, seized or confiscated property are regulated in more detail in the Decree on Procedure of Management of Forfeited Items, Assets and Securities (for criminal proceedings) and the Decree on procedures of Safekeeping, Management and Sale of Assets of Illegal Origin (for civil proceedings). However, Slovenia does not have a comprehensive system in place for the effective management over time of complex assets, such as active corporate ones.

Weighting and Conclusion

56. Slovenia mostly meets criteria 4.1 and 4.2, meets 4.3 and partly meets 4.4. The legal framework of the confiscation regime in criminal proceedings is comprehensive, and Slovenia has introduced legal grounds for civil forfeiture in 2011. Asset tracing measures and provisional measures for instrumentalities are not explicitly regulated although authorities believe that sufficient measures are available. The confiscation of instrumentalities from third parties is subject to specific conditions. The concerns under R.5 relating to the funding of individual terrorists and terrorist organisations are also relevant here. There are no comprehensive mechanisms in place to manage assets. **Slovenia is LC with R.4.**

Recommendation 5 - Terrorist financing offence

57. In the 2010 MER, Slovenia was rated largely compliant on former SR. II. Slovenia had not criminalised FT as broad as required by the UN FT Convention and there was no separate incrimination of the financing of an individual terrorist or terrorist organisation.

58. *Criterion 5.1* - Art. 109 (1) CC criminalises anyone who provides or collects money or property in order to partly or wholly finance the committing of offences under Art. 108 (Terrorism [including participation in a terrorist organisation]), Art. 110 (Incitement and public glorification of terrorist activities) and Art. 111 (Conscripting and training for terrorist activities). The list of terrorism actions of Art. 108 criminalises most but not all of the elements of the offences in the treaties listed in the Annex to the FT Convention. Moreover, the offences under Art. 108 carry an additional purposive element (intention to destroy or severely jeopardise the constitutional, social, or political foundations of the Republic of Slovenia or another country or international organisation, to raise fear among the population or to force the Government of Slovenia or another country or international organisation to perform or stop performing something). Slovenia has ratified or acceded to all the Conventions and Protocols in the Annex to the FT Convention and has criminalised the relevant offences in line with the treaties without a purposive element, but its FT offence does not apply to these offences.

59. *Criterion 5.2* - The FT offence does not criminalise the financing of a terrorist group or an individual terrorist if the intention of the financier for the collection or provision of the funds was not directed at the committing of terrorist offences proscribed by Art. 108, 110 and 111 CC. The financing of terrorist groups and terrorist individuals operating within terrorist groups is partially covered by the link between the FT offence and Art. 108 (7) and (8), as a result of which is criminalised the funding of any person's participation in and establishment and leading of a terrorist organisation or group which has the intention to commit terrorist offences. The wording 'in order to' in Art. 109 means that intention for use of funds for terrorist acts must be proven, and only knowledge is not enough.[70]

60. *Criterion 5.2bis* - If it can be proven that the financier of travel costs had the intention to fund the perpetration of terrorist acts covered by Art. 108, which include participation in a terrorist organisation, or the provision of terrorist training covered by Art. 111 CC, the regular FT offence could apply. In other cases, the financing of terrorist travel is not criminalised. Slovenia has signed

[70] Law on Amendments to the Criminal Code which includes also amendments to Art. 108, 109, 110 and 111 CC is in the legislative procedure.

the Additional Protocol to the Council of Europe Convention for the Prevention of Terrorism which includes such criminalisation, and is in the process of amending the CC to proceed with the ratification.

61. *Criterion 5.3* - The wording “money or property” in the FT offence does not specify a source, so it can be concluded that it refers to any funds or other assets whether from legitimate or illegitimate source. The terms are not defined in the law but seem sufficiently broad to cover any kind of funds or other assets, which was confirmed on-site in discussions with judicial authorities.

62. *Criterion 5.4* - The same penalty for FT is prescribed if the money or property provided or collected was not actually used for committing the criminal acts (Art. 109 (2)). The formulation of Art. 109 does not explicitly require that the provided or collected funds were linked to a specific terrorist act. However, in the absence of case law, discussions with practitioners met on-site could not fully reassure the assessment team that the intention of the financier that would need to be proven is the general intention for funds to be used for terrorist offences, and not for an exactly specified terrorist act that is at least in its preparatory phase. Furthermore, the FT offence does not criminalise the financing of a terrorist group or individual if the purpose for which the terrorist financier intended those funds or other assets provided to individual terrorists or terrorist groups was not directed at the committing of terrorist offences of Art. 108, 110 and 111 CC. As described under c.5.2, the funding of someone’s participation in a terrorist group or establishment or leadership thereof is criminalised, but the financing of individual terrorists and terrorist groups in other circumstances is not criminalised.

63. *Criterion 5.5* - The law does not expressly state that it is possible for the intent and knowledge to be inferred from objective factual circumstances. In general, the principle of free evaluation of evidence (Art. 18 CPC) would enable judges to make such inference.

64. *Criterion 5.6* - Natural persons convicted of FT are subject to imprisonment from one to ten years. A more severe penalty is prescribed if an offence was committed within a terrorist organisation or group to commit terrorist acts: imprisonment between three and fifteen years. The judge has discretion to determine the sentence within this range based on proportionality considerations, considering all mitigating and aggravating circumstances, including the degree of criminal culpability and motives for the offence (Art. 49 CC). Confiscation of proceeds of crime is mandatory (Art. 74 CC). The applicable sanctions are proportionate and dissuasive.

65. *Criterion 5.7* - Legal persons may be liable for the FT criminal offence (Art. 42 CC; Art. 25 LLPA). The liability of a legal person does not preclude the criminal liability of natural persons or responsible persons for the committed criminal offence (Art. 5(2) LLPA). The available punishments appear proportionate and dissuasive (Art. 12, 13, 16 and 26 LLPA).

66. *Criterion 5.8* - There are appropriate ancillary offences to the FT offence, including attempt, participation as an accomplice and organising or directing others (Art. 20 and 34 CC). Art. 294 CC prescribes the offence of participation in a criminal association.

67. *Criterion 5.9* - FT is a predicate offence for ML. Slovenia uses an “all crimes approach” for ML.

68. *Criterion 5.10* - Pursuant to the general provisions of the CC on jurisdiction (Art. 10 – 14), the FT offence applies regardless of whether the person committing the offence is in the same country as the relevant terrorist, terrorist organisation, or terrorist act.

Weighting and Conclusion

69. The FT offence is not broad enough to cover the financing of all acts which constitute an offence within the scope of and as defined in the treaties listed in the annex to the FT Convention. Furthermore, it does not cover the financing of a terrorist group or an individual terrorist for a purpose other than the committing of terrorist offences. **Slovenia is PC with R.5.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

70. In the 2010 MER, Slovenia was rated partially compliant with then SR.III. The procedures for freezing of terrorist funds and related procedures had not been fully elaborated nationally and were not publicly known. There was a lack of guidance and training.

71. Slovenia implements UNSCRs 1267/1989 and 1988 and 1373 primarily through EU mechanisms. The Act relating to Restrictive Measures Introduced or Implemented in Compliance with Legal Instruments and Decisions adopted within International Organisations (hereafter: ARM) represents a basic national framework for implementation of targeted financial sanctions (TFS), in some aspects complementing EU regulations. Under Art. 3(1) ARM, the Slovenian Government has issued decrees to facilitate the implementation of the EU Regulations.[71] The ARM also provides a legal basis for the Government to make domestic designations, although this power has never been used.

72. *Criterion 6.1* - Slovenia implements UNSCRs 1267/1989 and 1988 primarily through two European Council Regulations which have direct effect in all EU member states: 753/2011 on Afghanistan and 881/2002 (amended by 754/2011) on Al Qaida.

a) The Slovenian Government established the Sanctions Coordination Group (SCG) with a purpose of monitoring and coordinating the implementation of restrictive measures (Art. 7(1) ARM; Art. 2 Act Establishing a Permanent Coordination Group for Restrictive Measures). The SCG is chaired by the MFA and composed of representatives of various Ministries, the BoS, the FARS, SISA, the Nuclear Safety Administration, and OMLP. Its functioning is governed by internal Rules of Procedure (RoP). On 26 October 2016, the Group adopted an Annex to its RoP. Chapter I of the RoP Annex sets out tasks regarding national designation proposals; and Chapter II specifies that Chapter I will be applied *mutatis mutandis* when making proposals to the UNSC. Accordingly, the SCG is responsible to propose designations to the Government, and the MFA sends the proposal to the UNSC upon decision by the Government.

b) The RoP do not contain specific references to the listing criteria of relevant UNSCRs. As described above, the RoP Annex states in Chapter II that Chapter I will be applied *mutatis mutandis* when proposing to list on the UNSC counter-terrorism sanctions list. Chapter I contains the EU listing criteria, which are in line with those of the UNSC.

c) The RoP Annex states that a designation proposal to be discussed within the SCG must be duly substantiated, and shall be deemed as such if it meets the criteria under the APMLFT or the CPC, in particular when adequate measures have already been taken under those acts such as a temporary freezing of suspicious transactions, for which reasonable grounds of suspicion suffice.

d) Slovenia has not made any proposal; hence it has not had to put into practice the procedures and standard forms for listing adopted by the 1267/1989 or 1988 Committees.

e) SCG designation proposals to the Government must be accompanied by a detailed statement of reasons (RoP Annex). It is not explicitly mentioned whether this statement would be forwarded to the UNSC, and whether it would be specified if Slovenia's status as designating state may be known.

73. *Criterion 6.2* - Slovenia implements designations pursuant to UNSCR 1373 primarily through EU Council Common Position (CP) 2001/931/CFSP on criteria for listing and Regulation 2580/2001 on application of restrictive measures to listed persons and entities. The domestic powers under the ARM which could also be relevant for implementing UNSCR 1373 have never been used.

---

[71] Decree on restrictive measures against certain persons and entities associated with the Al-Qaida network and on implementation of Council Regulation (EU) No 881/2002 (OJ RS 20/13); Decree on restrictive measures against certain individuals, groups, undertakings and entities in view of the situation in Afghanistan and on implementation of Council Regulation (EU) No 753/2011 (OJ RS 20/13); Decree on Restrictive Measures for the Fight against Terrorism and Implementation of the Decree of the Council (ES) No. 2580/2011 (hereafter: 2580/2001 Decree).

a) At the EU level, the Council CP 931 Working Party (WP) is the competent authority for making designations based on a prior decision by a competent national authority in a Member State or a third state. The competent Slovenian authority for submitting proposals to the CP 931 WP is the MFA. Domestically, the Government can issue regulations introducing restrictive measures including in cases where no international obligation exists to do so, based on a proposal by the SCG upon motion of Group members, EU member states or third states (Art. 2 – 3 ARM; RoP Annex).

b) At EU level, identification of designation targets is covered by CP 2001/931/CFSP. The RoP Annex describes mechanisms for submission and consideration of national-level proposals.

c) When requests from third states to the EU are received, the CP 931 WP examines whether the designation criteria of CP 2001/931/CFSP, which are compliant with UNSCR 1373, are met. At the national level, SCG members have 15 days to check the material from a proposing party. Exceptionally, the proposing party may put forward a justified request to shorten the deadline. After the given time has passed, the Group must issue a written opinion together with a statement of reasons for designation. The MFA would submit this to the Government and prepare a legal act if decision for designation is made. In the absence of practice and further specification of deadlines, no conclusion can be drawn regarding prompt evaluation of requests.

d) The CP 931 WP applies a "reasonable basis" evidentiary standard of proof for designation decisions, which are not conditional on the existence of criminal proceedings (Art. 1(2) and (4) CP 2001/931/CFSP). The national framework refers to the criteria of the EU CP, the APMLFT and the CPC, which indicates that designations shall not be conditional upon criminal proceedings.

e) There is no EU mechanism to request third countries to give effect to EU TFS, nor is there any such specific procedure under domestic law in relation to actions initiated under Slovenian freezing mechanisms. In practice, at the EU level, some countries (notably those in the process of becoming EU members) are invited to abide by all new CFSP decisions. All designations must be sufficiently substantiated to identify the person to be designated (Art. 1(5) 2001/931/CFSP).

74. *Criterion 6.3*

a) All EU member states are required to provide each other with the widest possible range of police and judicial assistance in preventing and combating terrorism, inform each other of any measures taken, and cooperate and supply information to the relevant UN Sanctions Committee (Art. 8 Reg. 881/2002; Art. 8 Reg. 2580/2001; Art. 4 CP 2001/931/CFSP). The national legal framework does not prescribe specific authorities or mechanisms to collect or solicit information to identify targets for designation. In the RoP Annex, it is specified that all SCG members, which include OMLP and SISA, can submit designation proposals. The APMLFT lists which types of information gathered by the OMLP can be shared within the SCG, which appears to be an adequate list (Art. 118, 136). Proposing parties and SCG members will inform each other about any new facts and developments with regard to listings. The SCG can ask for additional information and can invite representatives of organs and organisations to attend its meetings to present background information in order to facilitate discussion on designation (RoP Annex).

b) EU designations take place without prior notice to the person/entity (Reg. 1286/2009 preamble para. 5). For designations, the Court of Justice of the EU makes an exception to the general rule of prior notice for decisions in order not to compromise the effect of the freezing order. The RoP Annex for the SCG does not contain any rules on involving the subject of listing proposals in its national decision-making process and stipulates that the MFA will inform each entity listed *after* a listing decision has been taken. It can thus be inferred that authorities can act *ex parte*.

75. *Criterion 6.4* - A delay arises between the date of a designation by the UN Committees and the date of its transposition into EU law, due to time taken for consultation and translation of the legal act into 24 European languages. An expedited procedure has been adopted by the European Commission for implementation of new listings by the 1267/1989 (Al Qaida) Committee which has closed the gap from 7-29 days in 2013 to approximately 4-12 working days in 2015 and 3-9 working

days in 2016. This is however still not consistent with the requirement to implement sanctions without delay. Furthermore, the transposition of 2 designations by the 1988 (Taliban) Committee in 2015 took 15 and 127 days respectively. On the basis of the ARM, the Slovenian government could ensure that new UNSC listings come into effect faster; however there has been no practice to date to adopt national measures before EU legal acts. The APMLFT could also be used to some extent to mitigate the effects of delays: its gives the OMLP the power to temporarily suspend transactions for up to three working days on its own initiative or upon request of foreign counterparts in case of reasonable suspicion of FT (Art. 96, 110). The Police and Prosecutors could then apply for a court order for further temporary freezing. However these measures, which are limited and connected to the criminal procedure, cannot be understood as implementing the standard.

76. For EU-level designations based on UNSCR 1373, TFS are implemented without delay because Regulation 2580/2001 is immediately applicable in all EU member states. In the absence of autonomous TFS issued at national level and clear deadlines under the law, there is no information available as to timeliness of implementation under the domestic legal framework.

77. *Criterion 6.5*

a) For UNSCRs 1267/1989 and 1988 as transposed by the EU Regulations, there is an obligation to freeze all funds, financial assets, or economic resources of designated persons/entities. However, as described under c.6.4, there are delays in transposition which can further result in *de facto* prior notice to the persons or entities concerned. For UNSCR 1373, the obligation to freeze all funds/assets of designated persons/entities applies immediately and without notice in all EU member states (Art. 2(1)(a) Reg. 2580/2001). Listed EU 'internals' are not subject to freezing measures but only to increased police and judicial cooperation among member states (CP 2001/931/CFSP footnote 1 of Annex 1). In Slovenia, the freezing obligations of Regulation 2580/2001 apply however also to internal terrorists designated by the EU, as articulated since March 2013 in Art. 2 of the Slovene 2580/2001 Decree. The Decrees adopted by Slovenia to facilitate the implementation of the EU Regulations further prescribe misdemeanour sanctions for failure to freeze funds of designated persons and entities.

Governmental regulations introducing domestic restrictive measures would specify on a case-by-case basis their type and implementation method, supervision and sanctions for violations (Art. 3(1) ARM). In the absence of practice and more detailed legal provisions, it is not possible to evaluate the freezing obligations to be articulated in such regulations.

b) For UNSCRs 1267/1989 and 1988, the EU legal framework ensures that the freezing obligation extends to all funds/other assets that belong to, are owned, held or controlled by a designated person/entity, including assets of a third party acting on their behalf or at their direction (Art. 2(1) Reg. 881/2002 as amended by Reg. 2016/363; Art. 3(1) Reg. 753/2011). For UNSCR 1373, the EU freezing obligations do not explicitly cover funds controlled by or indirectly owned by, or derived from assets owned by a person acting at the direction of designated persons/entities (Art. 2(1)(a) Reg. 2580/2001). However, Art. 2(3) (iii) and (iv) of the Regulation empower the Council to designate any legal person, group or entity controlled by a designated subject, or a natural person acting on behalf of a designated subject, which largely addresses the gaps.

c) EU nationals and persons within the EU are prohibited from making funds and other assets available to designated subjects (Art. 2(2) Reg. 881/2002, Art. 4 Reg. 753/2011). Furthermore, according to Art. 374a of the Slovenian CC, whoever enables access to property in contravention with restrictive measures shall be sentenced to between six months and five years in prison.

d) All EU regulations are published in the Official Journal of the EU, and the EU maintains a consolidated list of designated individuals. The EU also provides for the possibility to subscribe to an RSS feed in order to be informed automatically of all changes. Slovenian authorities have issued Guidelines on the implementation of financial restrictive measures (hereafter: FRM Guidelines). However, they address only FIs and not DNFBPs and are contrary to the standard as regards the moment of freezing the funds in cases of possible matches (when not all indicators are met). FIs are

advised to notify the MFA in case of a possible match and to await the MFA's assessment of whether it is an actual match, before freezing the funds. The guidelines also do not include information on freezing obligations for EU internals.[72]

e) Natural and legal persons (including FIs/DNFBPs) are required to provide immediately any information about accounts and amounts frozen under EU legislation to national competent authorities (Art. 5.1 Reg. 881/2002; Art. 4 Reg. 2580/2001; Art. 8 753/2011). For Slovenia, the competent authority is the MFA. The FRM Guidelines give the specific contact details for the MFA. The EU implementing Decrees adopted by Slovenia prescribe misdemeanour sanctions for not immediately sending all information to the competent authority.

f) The EU framework for UNSCR 1267 protects the rights of bona fide third parties acting in good faith when undertaking freezing actions (Art. 6 Reg. 881/2002; Art. 7 Reg. 753/2001). The ARM renders impossible compensation of damage caused through lawful implementation of sanctions (Art. 9). This also explicitly applies to implementation of sanctions based on directly applicable EU legal acts, filling any possible gaps in the EU framework which does not have an explicit clause for protection of bona fide third parties in the context of UNSCR 1373.

78. *Criterion 6.6*

a) The Annex to the RoP of the SCG outlines procedures for the SCG to propose de-listings from UNSC lists in case the criteria for designation of persons and entities are not or no longer met. However the Annex is not (yet) publicly available.

b) The EU WP revises the list of EU-level designations pursuant to UNSCR 1373 at regular intervals to examine whether grounds remain for keeping a subject on the list (Art. 6 CP 931/2002). Independently of this review, listed subjects, a member state or the third state which had originally proposed the listing in question can make a request for de-listing at any time. The General Secretariat of the Council acts as a mailbox for de-listing requests, and requests are discussed in the CP 931 WP. Amendments to Regulation 2580/2001 are immediately effective in all EU member states. The Slovene FRM Guidelines refer to available guidance at EU level and indicate that, pursuant to EU legislation, requests for de-listing should be submitted to the EU Council.

The FRM Guidelines do not contain any guidance on de-listing for national measures. The RoP Annex does set out a procedure for delisting from the national list by the SCG. Requests can be made anytime by listed persons, groups and entities, by submission of supporting information to the MFA, and will be discussed in the Group as a matter of priority. However, as noted above, the Annex is not (yet) publicly available.

c) Designated persons or entities may institute proceedings before the Court of Justice of the EU to challenge the relevant EU measures (Art. 263 para 4 and Art. 275 para 2 Treaty on the Functioning of the EU). At the national level, authorities have advised that challenges can be filed at the Administrative Court against a government regulation containing a designation on the basis of the Administrative Dispute Act. This law provides for judicial review of governmental acts which encroach on the legal position of the plaintiff or infringe on human rights and fundamental freedoms of the individual, if no other judicial protection is available.

d) & e) For designations pursuant to UNSCR 1267/1988 and 1989, subjects are notified of their designation and the reasons and legal consequences and have the right to request a review. There are EU-level procedures for de-listing names, unfreezing funds and reviewing designation decisions by the EU based on UNSC listings. At the UN level, the review can be brought before the

[72] The Sanctions Coordination Group adopted an amended version of the FRM Guidelines on 26 October 2016, which does include information on freezing obligations for EU internals. However at the time of the on-site visit this version was not yet made available to the public. After the on-site visit the new version has been published on the MFA's website.

Ombudsperson (for UNSCR 1989), or before the UN Focal Point (for UNSCR 1988). The FRM Guidelines also refer to the UNSC Focal Point and Ombudsperson mechanisms.

f) Slovenia appears not to have publicly known procedures to unfreeze the funds of persons inadvertently affected. The FRM Guidelines prescribe that in order to *avoid* unnecessary or erroneous freezing, the following procedure is recommended: in case of a suspected match with the EU lists, the MFA should immediately be notified. The MFA, through SCG members, will try to establish whether there is an actual match between the names or it is a case of a "false positive". In such cases pending transactions may only be carried out after a positive opinion is obtained from the MFA. If the assessment indicates that a customer or company matches a person or a company on the list, the credit or financial institution must freeze the funds immediately in compliance with the EU Regulation. These provisions appear not to apply to DNFBPs and their effect on the timeliness of freezing is questionable (see under c.6.5(d)).

g) For the EU framework, the communication framework regarding de-listing and unfreezing is the same as described under c.6.5(d). The ARM instructs the Government to publish a notification of the termination of restrictive measures imposed by the UN and EU in the Official Gazette. The Slovenian authorities do not seem to use other mechanisms for active and immediate communication to FIs and DNFBPs or for providing guidance on obligations to respect a de-listing or unfreezing action.

79. *Criterion 6.7* - At the EU level, there are mechanisms for authorizing access to frozen funds or other assets which have been determined to be necessary for basic expenses, the payment of certain types of expenses, or for extraordinary expenses (Art. 5 Reg. 753/2011, Art. 5–6 Reg. 2580/2001). The Annexes to EU Regulations 753/2011 and 2580/2001 and the Slovene implementing Decrees specify that the Ministry of Finance is the competent authority in Slovenia to decide on such release of funds. Art. 8 ARM prescribes that for applications of persons filed on the basis of the ARM, including in relation to directly applicable EU Regulations, the general administrative procedure shall apply. The Article also specifies the decision-making process, which can include a request by the responsible Ministry for the advice of the SCG.

Weighting and Conclusion

80. Slovenia meets criterion 6.7 and mostly meets criteria 6.2 and 6.3, whilst criteria 6.1, 6.4, 6.5 and 6.6 are partly met. Slovenia does not implement sanctions under UNSC resolutions without delay due to the overreliance on EU framework. The recent adoption of an Annex to the Rules of Procedure for the SCG with more detailed designation procedures is a welcome development. However some gaps remain and the Annex does not contain explicit references in relation to listings by the UNSC Committees. There are no national procedures for unfreezing requests, and national procedures for delisting requests are not publicly known. **Slovenia is PC with R.6.**

Recommendation 7 – Targeted financial sanctions related to proliferation

81. This recommendation was added to the FATF Standards in 2012. Slovenia has, therefore, not previously been assessed against this recommendation.

82. Slovenia primarily relies on EU legislation for the implementation of R.7. UNSCR 1718 concerning the DPRK is transposed into European law by Common Position 2006/795, Regulation 329/2007, and Council Decision 2013/183/CFSP. UNSCR 1737 concerning the Islamic Republic of Iran is transposed into European law by Regulation 267/2012 and Council Decision 2010/413. To facilitate the implementation of these Regulations, the Slovenian government has issued two Decrees under Art. 3(1) of the ARM.[73]

83. *Criterion 7.1* - R.7 requires the implementation of TFS without delay, meaning ideally within a few hours. As is the case for R.6, there are delays in the transposition of UN designations into

---

[73] Decree on restrictive measures against Iran and on the implementation of Council Regulation (EU) No 267/2012; Decree on restrictive measures against the Democratic People's Republic of Korea and on the implementation of Regulations (EU) as regards these restrictive measures.

European law. The problem is alleviated in the case of TFS related to proliferation, because new UN designations are rare and where they occur, it is frequently the case that subjects had already previously been listed by the EU. Theoretically, the Slovenian government could cover the time span between UN designation and EU transposition if necessary by issuing a regulation on the basis of the ARM.

84. *Criterion 7.2*

a) EU Regulations are applicable to all EU citizens and legal persons established under the law of a Member State or associated with a commercial transaction carried out in the EU (Art. 49 Reg. 267/2012; Art. 16 Reg. 329/2007). The freezing obligation is immediately activated upon publication of the regulations in the EU Official Journal. The delays in transposition of UN designations make that the obligation to execute freezing measures without delay and without prior notice is not complied with if entities have not previously been listed by the EU.

b) The EU freezing obligation applies to all types of funds as required by the standard.

c) The EU Regulations prohibit making available, directly or indirectly, funds or economic resources to designated persons or entities or for their benefit, unless otherwise authorised or notified in compliance with the relevant UN resolutions (Art. 6(2) Reg. 329/2007; Art. 23(3) Reg. 267/2012).

d) Regulations containing designations are published in the Official Journal of the EU. The EU also maintains a publically available on-line consolidated list and has published Best Practices for the effective implementation of restrictive measures. On the national level, the Slovene Guidelines on Financial Restrictive Measures (FRM Guidelines) prescribe the restrictive measures against third countries as all other restrictive measures which are not related to terrorism and which are associated with third countries including Iran and DPRK. The Guidelines do not however explicitly mention PF issues. Furthermore, they only address FIs, not DNFBPs, and appear contrary to the standard regarding the moment of freezing in case of suspected matches when not all indicators are met (see c.6.5(d) under R.6).

e) All natural and legal persons must immediately provide all information that will facilitate observance of the EU regulations, including information about the frozen accounts and amounts, to the competent authority as indicated in the Annexes to the Regulations (Art. 10(1) Reg. 329/2007; Art. 40(1) Reg. 267/2012). For Slovenia, this is the MFA. In addition, the EU Regulation on the DPRK instructs FIs, in the framework of their dealings with FIs domiciled in the DPRK or their branches and agencies abroad, that if they suspect or have good reason to suspect that funds are associated with PF, they should quickly report to the FIU or to another competent authority (Art. 11a Reg. 329/2007). Slovenia has again designated the MFA as the competent authority here (Art. 4(1)(e) DPRK Decree), although this will be changed to the Ministry of Finance (OMLP) once a planned new version of the DPRK Decree comes into force.[74]

f) The rights of bona fide third parties are protected (Art. 11 Reg. 329/2007; Art. 42 Reg. 267/2012; Art. 9 ARM).

85. *Criterion 7.3* - EU member states are required to take all necessary measures to ensure that the EU TFS are implemented and to determine a system of effective, proportionate and dissuasive sanctions (Art. 14 Reg. 329/2007; Art. 47 Reg. 267/2012). Art. 10 ARM prescribes that supervision of the implementation of international restrictive measures shall be carried out by public authorities as specified in the regulations issued on the basis of the Act and in accordance with the regulations governing their individual supervisory fields. The Iran and DPRK Decrees issued by the Slovenian Government specify the applicable misdemeanour sanctions for non-compliance with freezing obligations, and list bodies responsible for supervision albeit not in a very specific way ('the competent inspection and customs authorities, the police, and the competent holders of public authority' (…) 'within their subject-matter jurisdiction'). Criminal sanctions are prescribed by Art

[74] The Decree came into force on 15 April 2017 (OJ RS 18/17), see new Art. 5(1)(c).

374a CC for the offence 'Violation of restrictive measures' (imprisonment between six months and five years).

86. *Criterion 7.4* - The EU Regulations establish measures and procedures for submitting de-listing requests in cases where the designated subjects do not meet or no longer meet the designation criteria. The FRM Guidelines prescribe that requests for removal from lists related to the EU autonomous restrictive measures should be submitted to the EU Council General Secretariat and are processed in line with Annex I of the EU Guidelines. Requests for removal from lists related to UNSC resolutions may be submitted directly to the relevant UNSC Sanctions Committee via the UNSC focal point or via the MFA.

a) The EU Council communicates its designation decisions, including the grounds for inclusion, to the designated subjects which have the right to comment on them. If this is the case or if new substantial proof is presented, the Council must reconsider its decision. Individual de-listing requests must be processed upon receipt, in compliance with the applicable legal instrument and EU Best Practices. Designated subjects are notified of the Council decision and can use this information to support a de-listing request filed with the UN (notably via the Focal Point established pursuant to UNSCR 1730/2006). When the UN decides to de-list a person, the European Commission modifies the EU lists without the subject in question having to request it (Art. 13.1 (d) and (e) Reg. 329/2007; Art. 46 Reg. 267/2012). The listed persons or entities can also file an appeal with the European Court of Justice to challenge the listing decision. The FRM Guidelines contain some information to the public on how to proceed with both UN and EU de-listing requests.

b) Slovenia does not appear to have publicly known procedures for unfreezing the funds of persons inadvertently affected by a freezing mechanism. See however the analysis under R.6, c.6.6(f), on the procedure in place to avoid unnecessary or erroneous freezing according to the FRM Guidelines.

c) At the EU level, there are procedures for authorizing access to funds or other assets if member states' competent authorities have determined that the exemption conditions of UNSCRs 1718 and 1737 are met (Art. 7 Reg. 329/2007; Art. 26-28 Reg. 267/2012). Slovenia has appointed the Ministry of Finance as the competent authority for this matter (Art. 4(1)(b) DPRK Decree; Art. 5(1) Iran Decree). Further publicly known domestic procedures are set out in the FRM Guidelines.

d) EU communication mechanisms in case of de-listing are the same as described under c.7.2(d). Furthermore, the ARM instructs the Government of Slovenia to publish a notification of the termination of UN and EU restrictive measures in the Official Gazette. Such notice was indeed published within a day when EU Regulation 267/2012 on Iran was significantly amended in January 2016. It appears that Slovenian authorities have not elaborated other mechanisms for immediate communication to FIs and DNFBPs or guidance on obligations to respect de-listing or unfreezing actions.

87. *Criterion 7.5*

a) Interests or other earnings to frozen accounts or payments due under contracts, agreements or obligations are permitted, as long as they are subject to the freezing action (Art. 9 Reg. 329/2007; Art. 29 Reg. 267/2012). Financial or credit institutions must provide information on such transactions without delay to BoS (Art. 4(1)(d) DPRK Decree; Art. 5(1) Iran Decree).

b) Payments due under a contract entered into prior to the date of listing are permitted provided that prior notification is made to the UN Sanctions Committee and that it is determined that the payment is not related to any of the prohibitions under the regulations (Art. 8 Reg. 329/2007; Art. 25 Reg. 267/2012). Slovenia has appointed the Ministry of Finance as the competent authority that must decide on such releases of funds (Art. 4(1)(d) DPRK Decree; Art. 5(1)) Iran Decree).

Weighting and Conclusion

88. Concerns expressed under R.6 relating to delays in implementation of TFS are also relevant to this Recommendation. **Slovenia is PC with R.7.**

Recommendation 8 – Non-profit organisations

89. In the 4th round, Slovenia was rated partially compliant with then SR.VIII. It was unclear whether there was coordination between different governmental actors in assessing sector risks; there was no fully comprehensive review of NPOs or outreach undertaken; no "know your beneficiary and associate" rules; and supervision was assessed as insufficient. Since the 4th round, the standard has changed considerably, especially by clarifying the application of the risk-based approach to NPOs.

90. NPOs in Slovenia can take different legal forms. The sector includes around 31,500 individual NPOs, of which about 74% are associations (also often referred to as 'societies'), 10% are institutes, 4% are religious communities and 1% are foundations. Humanitarian organisations (HO) are associations with a special status, granted by ministries in accordance with the Humanitarian Agencies Act. The main benefit of the status is access to special public funds and possibility to distribute funds to individuals untaxed. Other NPOs may also disburse financial aid to individuals, but recipients would have to pay income tax, which is why this is uncommon according to authorities.

91. *Criteria 8.1* - The authorities have undertaken several exercises to obtain insight in the NPO sector (in 2006, 2012 and in the course of the 2015-2016 NRA). However, as described under IO.10, the evaluation team found no evidence that these exercises set out to identify features and types of NPOs likely to be at risk for FT or led to real insight in the FT risks in the sector. Action taken pursuant to the analyses has been limited or is still in development. The Action Plan following the 2015-2016 NRA contains some broad measures for the NPO sector which do not appear to be based on an understanding of those NPOs that may be at risk for FT.

92. According to the authorities, there is a good basis for reassessing the sector periodically by reviewing and processing information annually provided by NPOs. Indeed, the annual reporting obligations described under c.8.3 below, general procedures for inspection by tax authorities and powers under the criminal procedure can enable further review of features and types of NPOs that are at risk of being misused for FT. Yet concerns remain with regard to whether relevant analysis follows after the receipt of this data and whether new information may trigger reassessments of potential FT vulnerabilities.

93. *Criterion 8.2*

a) The Office for NGOs within the Ministry of Public Administration defines transparency of the NGO sector as a priority issue and funds relevant projects for quality certification since 2005 (see IO.10). Slovenia has mechanisms for ensuring transparency with regard to NPOs operating in the country through registration and annual reporting obligations (see c.8.3). Furthermore, the NPO umbrella organisation CISCD publishes a large amount of data on activities and incomes of the sector on its public website.

As recognised by the authorities, there is still place for improvement, for example with respect to publication of founding acts of associations and foundations as well as publication of annual reports of institutes and foundations, which may enhance integrity and public confidence in the sector. Currently, these acts and reports are available to everyone upon request, but private persons must pay a small fee to obtain them.

b) No specific outreach to the NPO sector or the donor community on FT issues has been conducted.

c) No best practices have been developed in cooperation with NPOs to protect them from FT abuse.

d) Provisions of the APMLFT (Art. 67) and Tax Procedure Act seek to limit the use of cash by legal persons. Furthermore, in January 2016, the Law on fiscal verification of invoices was amended to ensure that any 'business entity', including NPOs, dealing with cash must have an electronic device which is connected to Tax authorities and whose use is required in order to receive valid receipts for cash payments. Furthermore, since January 2016, the Act on fiscal verification of invoices is in force

which binds all business entities, including NPOs, to use an electronic device for the issuance of receipts or invoices, connected to the central information system of the tax authority, when they accept payments in cash. This system is on-line connected to the FARS and provides the FARS with data on every invoice paid in cash and enables it to have a control over cash transactions (payments for goods and services) in the economy.

94. *Criterion 8.3 -* The Interpretative Note to R.8 lists various measures that could be applied to NPOs, in whole or in part, depending on the risks identified. Slovenia does not apply a risk-based approach but applies the following measures to all main types of NPOs:

i. Foundations, institutes and associations are subject to registration requirements and obtain legal personality upon registration. Religious communities can choose if they want to be registered in order to obtain legal personality, but they can also exercise their activities directly on the basis of the constitution. The registration of **associations** and their affiliates is regulated in the Associations Act (AA) and falls within the competence of local administrative units in whose area of jurisdiction an association has its head office. They are recorded in the Register of associations. **Foundations** need the approval of the competent authorities (the Ministry competent for the field in which the particular foundation operates) for their establishment on the basis of the Foundations Act (FA) and are recorded in the Register of foundations. **Religious communities**, governed by the Freedom of Religion Act (FRA), are registered by the Office for religious communities of the Ministry of Culture and entered in the register of Religious communities. **Institutes** are registered by the District Courts in accordance with the Institutes Act (IA), the Court Register Act and the Decree on the registration of companies and other legal entities in the register of companies. Information from all Registers is transferred to the Business Register of Slovenia, managed by APLRRS, which enables all public information on NPOs to be available at one place. Information that is collected and held by registering bodies but not made public in the registers is available to competent authorities with a legal interest.

ii. With their application for registration, associations, foundations, institutes and religious communities must provide personal information on founders and legal representatives and must enclose their charter, which includes information on the organizational structure and purpose of operations (Art. 9, 18 AA; Art. 6, 14 FA; Art. 8 IA; Art. 14 FRA). For foundations the charter also contains information on the first board of trustees. There is no obligation however on foundations to keep up-to-date information on the board of trustees when members change. The on-line public registers include the information on the representatives. Founding acts of institutes are published online in the Business Register; charters of associations and foundations are kept by authorities and available to the public upon payment of a small fee. There is no obligation for institutes to keep or make available up-to-date information on their council members.

iii. Under Art. 26 AA, **associations** must prepare an annual report including the balance sheet and internally audited financial statement including the actual statement of assets and the association's operations in accordance with accounting standards for associations (Slovene Accounting Standard 33 2006; renewed in 2016). When the statement of accounts exceeded 1 million EUR during the previous fiscal year, it must be externally audited (Art. 27 AA). According to Art. 30 FA, **foundations** shall keep books of account and produce annual reports in compliance with regulations specifying keeping of books of account and elaboration of financial reports for establishments (Accounting Act). The Body Competent for Foundations may request an external audit of financial management. **Institutes and religious communities** must also keep books of account and produce annual reports in compliance with Art. 20-29 of the Accounting Act. The financial statements of all NPOs must also be separately submitted to the FARS for taxation purposes.

iv. There are relevant legislative requirements on spending income only on the NPO’s stated purposes (Art. 24-25 AA, Art. 27 FA; Art. 18-21, 48(2) IA; Art. 20 Act on legal position of the religious communities).

v. There are no requirements on NPOs to take reasonable measures to confirm the identity, credentials and good standing of beneficiaries and associate NPOs and to confirm that they are not involved with or financially support terrorists or terrorist organisations.

vi. With regard to record-keeping, financial statements of all legal persons must be kept indefinitely under the Accounting Act. It appears that there are no obligations on NPOs to maintain for at least 5 years the information on purpose and objectives of their stated activities and of identity of the person(s) who own, control or direct their activities, including senior officers, board members and trustees. However, authorities advised that all relevant documents needed for registration and all data registered of NPOs are kept permanently by registering bodies.

95. *Criterion 8.4*

a) There is no single authority responsible for monitoring compliance by NPOs. The FARS is responsible for monitoring implementation of accounting provisions and has both off- and on-site inspection powers. The APLRRS is responsible for monitoring the submission of the annual reports for associations, foundations and institutes. The relevant registering bodies (listed under c.8.3(i)) can monitor compliance with registration and reporting obligations.

The Internal Affairs Inspectorate (IAI) of the Ministry of Interior further supervises (through off-site inspection) the tasks and activities of associations, requirements related to name, office and status, and requirements on the association's assets (prohibition to divide assets among members and obligation to spend surplus income to fulfil the purpose and objectives of the association), upon its own initiative or upon proposal of other authorities or anyone detecting violations (Art. 51 AA). It appears that for other NPOs, there are no bodies with powers to conduct such inspections.

Since there are no requirements with regard to beneficiaries and associate NPOs, these issues appear to fall out of the general supervision framework. It is unclear whether the supervisory measures provided for by the law allow for a risk-based, targeted approach to supervision.

b) Associations and foundations can be sanctioned for violations of requirements for book-keeping, annual financial reporting and communication of changes in registration data to competent authorities, and for performing activities in contravention to their charters (Art. 52-53 AA; Art. 35, 35a FA). Institutes can also be sanctioned for failure to communicate changes in registered data within 15 days (Art. 3(3), 53 CRA). Administrative sanctions for failure to communicate changes are very low (fines of 400-600 EUR for associations and foundations and 1,600 EUR for institutes). There appear to be no sanctions available on religious communities for failure to report changes in data that has been registered to competent authorities. The Accounting Act prescribes administrative sanctions in ranges of approximately 400 EUR to 25.000 EUR for all legal persons which provide false information in accounting records and who fail to submit annual reports (Art. 55 Accounting Act). Associations can be banned by court decision in case they engage in illegal activity or if they are operating for profit-making purposes (Art. 41 AA). NPOs as legal persons can also be held criminally liable for criminal offences under LLPCOA and criminal sanctions would be available which include fines of EUR 50,000 – 1,000,000 and winding-up.

96. *Criterion 8.5* - Authorities have access to information on NPOs through the collection by registering bodies of founding acts/charters and lists of founders. Authorities with a legitimate interest may request such information held by the registering bodies and by APLRRS. Annual reports of NPOs, as far as they are not already published online in the Business Register, are made available by APLRRS to authorities upon request. Since 2010, the APLRRS electronically transmits the annual reports of all legal entities, including NPOs, to the OMLP.

97. The APMLFT further provides for powers for the OMLP to analyse data, information and documentation on the basis of a reasoned written initiative by the IAI, as well as other inspection authorities responsible for supervision over the operation of NPOs when there are grounds to suspect ML or FT in connection with their operations, members or persons associated with them (Art. 99(2)). During the course of an investigation, LEAs can use investigative powers under the CPC

to search premises and seize documents. SISA also has expertise and capability to examine NPOs suspected to be linked to terrorist activity. There is a mixed CT working group within the National Security Council, composed of representatives from *inter alia* SISA, Ministry of Interior, Police, FARS and OMLP which has possibilities for information-sharing in case NPOs are suspected to be linked to terrorism or FT.

98. It appears however that there are no concrete mechanisms for more regular information-sharing between the various competent authorities involved in registration and supervision of NPOs in order to identify and monitor NPOs at risk when no concrete suspicions have arisen yet.

99. *Criterion 8.6* - Slovenia uses the general procedures and mechanisms for international cooperation to handle requests relating to NPOs, particularly through the OMLP.

Weighting and Conclusion

100. It appears that the major deficiencies identified through the 4th round evaluation have not been addressed. Although important mechanisms aimed at transparency in the sector are in place, national cooperation and coordination appear to be insufficient and not risk-based. This is particularly problematic given that responsibilities for registering and supervising NPOs in Slovenia are dispersed. The risk assessment of NPOs appears to be limited and no outreach programs on FT have been fulfilled. **Slovenia is rated PC with R.8.**

Recommendation 9 – Financial institution secrecy laws

101. Slovenia was rated as compliant in the 4th round MER. The FATF standards in this area have not been amended since then. However, the applicable law has changed and a new analysis has been undertaken.

102. *Criterion 9.1* - Slovenian legislation does not appear to inhibit the ability of competent authorities to access the confidential data and information held by FIs, and also exchange the relevant information both domestically and internationally. However, there is a lack of explicit exemptions from the principle of confidentiality where the sharing of information is required under R. 13, 16 and 17.

(a) *Access to information by competent authorities* - APMLFT provides for the clear exemption from the principle of confidentiality for FIs when data, information or documents are submitted to OMLP (Art. 126). Banks are also exempted from the confidentiality provisions when data is requested by a relevant supervisory authority or by a court, state prosecutor or police for pre-trial and criminal proceedings (Art. 126). Similar provisions are included in sector-specific legislation governing the activities of non-bank FIs (Art. 266 of the Insurance Act, Art. 79 of the Investment Funds and Management Companies Act, Art. 271 of the Financial Instruments Market Act and Art. 180 of the Payment Services and Systems Act). Furthermore, Criminal Procedure Code allows the investigating judge to require banks, savings banks or other savings-credit services to disclose confidential information based on a grounded request of the public prosecutor (Art. 156).

(b) *Sharing of information between competent authorities* - APMLFT provisions provide for the derogation to the principle of confidentiality that enables OMLP to cooperate with domestic supervisors, LEAs and foreign FIUs by exchanging relevant information (Art. 126-127). The same provisions exempt supervisors, LEAs and other state authorities from the confidentiality clauses when submitting relevant information to OMLP. BoS can also disclose confidential information to competent authorities domestically, including OMLP, supervisors and LEAs, and also those from EU Member States under Art. 16 of the Banking Act. As for exchanging information internationally, the Banking Act allows BoS to exchange confidential information with competent authorities of third countries based on an information-exchange agreement (Art. 19). Other sector-specific laws provide for general exemptions for supervisory authorities of non-bank FIs to disclose confidential information in carrying out their supervisory responsibilities (Art. 272 FIMA, Art. 80 IFMCA, Art. 267 IA, and Art. 180 PSSA).

(c) *Sharing of information between FIs* - APMLFT allows FIs to share information on STRs and other information submitted to OMLP, as well as transactions suspended temporarily or criminal proceedings launched against a customer with other FIs established in the EU Member States or their majority-owned subsidiaries in third countries (Art. 123). The Banking Act also allows banks to disclose confidential data to parent entities in relation to supervision on a consolidated basis, and in other instances provided by the law (Art. 126 of Banking Act). Similar provisions are found in the sector-specific legislation governing the activities of non-bank FIs (Art. 266 IA, Art. 271 FIMA, Art. 79 IFMCA, and Art. 180 PSSA). However, the absence of explicit exemptions from confidentiality clauses in relation to correspondent banking, wire transfers and reliance on third parties implies that FIs must act within the limits of the existing privacy laws, including by obtaining express written consent from customers to disclose their confidential data.

Weighting and Conclusion

103. **Slovenia is LC with R.9.** Absence of explicit exemptions from confidentiality provisions related to the exchange of information between FIs where this is required under R.13, R.16 and R17 affects the overall rating.

Recommendation 10 – Customer due diligence

104. In its 4th round mutual evaluation report Slovenia was found to be largely compliant with former R.5. The applicable law has changed, so the new analysis has been undertaken.

105. *Criterion 10.1* - Art. 64 APMLFT prohibits anonymous or fictitious accounts and all such existing accounts have reportedly been closed.

106. *Criterion 10.2* - APMLFT stipulates that CDD be carried out when entering into a business relationship; when carrying out a transaction of EUR 15000 or more in a single or evidently linked operation; when there are doubts about the veracity and adequacy of previously obtained customer or beneficial owner information; or where there is a suspicion of ML/FT regardless of the amount (Art. 17 and 19) APMLFT. APMLFT stipulates that CDD be carried out when entering into a business relationship; when carrying out a transaction of EUR 15000 or more in a single or evidently linked operation; when there are doubts about the veracity and adequacy of previously obtained customer or beneficial owner information; or where there is a suspicion of ML/FT regardless of the amount (Art. 17 and 19) APMLFT. Slovenia allows specific complete or partial exemptions from application of AML/CFT measures for certain FIs and DNFBPs (Art. 5, 6 and 22 APMLTF) in line with the FATF standards.

Wire transfers above applicable threshold

107. With regards to wire transfers above EUR 1,000, EU Regulation (EC) No. 1781/2006, which is directly applicable in Slovenia, requires that the financial institution identify and verify the identity of the originator (i.e. customer) of transactions above the applicable threshold, and in cases where there are several transactions of lower amounts that appear to be linked and together exceed the threshold. However, this requirement does not include the full range of CDD measures such as identifying and verifying the beneficial owner, etc.

108. *Criterion 10.3* - The APMLFT requires FIs to identify customers, including occasional customers (Art. 17 (1) point 2) and verify their identity using authentic, independent and objective sources (Art. 16 (1) point 1). For natural persons or their legal representatives, and for statutory representatives and authorised persons of legal entities, the information must be obtained through examination of the person's official personal identification document in his/her presence (Art. 23 (1), 24 (1), 25 (1)). Art. 3 point 47 stipulates that 'official personal identification' shall mean any valid authentic instrument bearing a photograph, issued by a competent authority, and deemed a public document as per the legislation of the issuing State. Art. 26 also includes the possibility of electronic identification without the customer's presence in which case the identification relies on a means of electronic identification of such a level of reliability that it requires the presence of the customer at the time of issuing and issued by an issuer of means of electronic identification with its

registered office in Slovenia, another EU Member State or a third country. Art. 27 includes the possibility of video-based identification. If identification and verification takes place according to the Art. 26 or 27, enhanced CDD must apply (Art. 26 (7) in combination with Art. 13 and Art. 14 (2); Art. Art. 27 (1) point 6).

109. *Criterion 10.4* - Art. 16 (2) of APMLFT requires FIs to verify that any person who acts on behalf of the customer has the right to representation or is authorised by the respective customer, and to verify the identification of any such person in accordance with the provisions of the APMLFT.

110. *Criterion 10.5* - Art. 16 APMLFT requires FIs to determine the beneficial owner of the customer in the course of CDD. Art. 33 defines beneficial owner as a natural person who ultimately owns or otherwise exercises oversight of a customer, or a natural person on whose behalf a transaction is carried out. See further under c. 10.10 below and under R.24 and 25 for an analysis of some gaps in the more specific definitions of beneficial owners for legal persons and arrangements stipulated in Art. 35, 36, 37 as compared to the standard.

111. Art. 43 stipulates how the financial institution verifies the identity of these beneficial owners using original or certified documentation from the business, court or other public register. The register of beneficial owners may also be consulted (which will be possible once that is set up, see under R.24), with the caution that the obliged persons may not exclusively rely on that register.

112. Although both Art. 16 and 33 contain reference to the beneficial owner of the 'customer', thus not excluding beneficial owners of natural persons from the definition there are serious doubts as to how the FIs shall understand this legal concept for the following reasons: a) unlike for beneficial owners of legal persons and foreign legal arrangements (Art. 35, 36, 37), there are no articles in the APMLFT outlining in more detail how the beneficial owner of a natural person shall be ascertained; b) The only specific requirement to identify and verify a beneficial owner of a natural person is when a natural person carries out an (occasional) transaction of EUR 15 000 or more (Art. 24 (2)) whereas the obliged entity shall obtain a statement from the customer on whether he is conducting business on his own behalf or on behalf of a third party; c) Art. 43 (2) determines that an obliged person shall not obtain data on the beneficial owner of the customer if the customer is a natural person not performing a gainful activity.

113. In the case mentioned above of occasional transactions of 15,000 EUR or more the FI shall determine and verify the third party's identity and obtain the required data. However it is not explicitly stated that this shall be based on reliable information sources.

114. *Criterion 10.6* - Art. 16, 17 and 18 APMLFT require FIs to obtain information on the purpose and intended nature of business relationship as part of the CDD process at the inception of the business relationship.

115. *Criterion 10.7* - Art. 16 APMLFT requires FIs to conduct regular monitoring of business activities undertaken by its customers as part of CDD. Art. 49 APMLFT determines that monitoring of customer activities, including the origin of assets, shall be done to verify that they are compatible with the purpose and intended nature of the business relationship and with the regular scope of business. Art. 49 also requires on going due diligence whose scope and frequency depends on consideration of the ML/FT risk factors as identified in the NRA (Art. 9) and in the internal risk assessment that the financial institution is obliged to perform (Art. 13). In addition to this, the update of customer data and documents is required at least once every 5 years from the last CDD if the customer has effected at least one transaction with the financial institution in the last 12 months.

116. *Criterion 10.8* - Art. 43 (1) APMLFT requires FIs to verify the data to the extent that they understand the ownership and control structure of the customer and that it is satisfied that it knows the identity of the beneficial owner, commensurate to the ML/FT risks in conducting business with the entity in question. In addition, Art. 16 (1) point 3 together with Art. 137 (1) point 4 APMLFT requires that when establishing a business relationship with a customer, information should be obtained on its activity.

117. *Criterion 10.9 -* Art. 137 (1) APMLFT, in conjunction with Art. 16, 25 and 28 set out the requirement to record and verify the name and address of the customer who is a legal entity. Furthermore, Art. 28 sets out that the determination and verification of the identity of the legal entity shall be done by inspecting original or certified documentation from the public registers submitted by the representative or authorised person of the legal entity (par. 1) and by inspecting original or certified documents and other business documentation (par. 4). This could encompass information on legal form, proof of existence and powers that regulate and bind the legal entity although this is not made explicit. There is no requirement for FIs to obtain the information on the names of persons holding senior management positions if they are not statutory representatives or authorized persons.

118. *Criterion 10.10* - Art. 16 and 34-36 APMLFT set out the requirement to identify the beneficial owners of a corporate entity or other legal person. The definitions of beneficial ownership appear broadly in line with criterion 10.10 (a), (b) and (c) (see Art. 35). However, for other legal persons (such as associations and foundations), there is the assumption in the law that the beneficial owner is any natural person representing such an entity, which does not appear in line with the standard (Art. 36 (1)).

119. *Criterion 10.11*- Art. 16 and 37 APMLFT require the identification and detail the method of verification regarding beneficial owners of foreign legal arrangements ('foreign legal trust, foreign foundation or similar foreign legal entity'). Art. 37 APMLFT defines beneficial owners of such arrangements as the settlor, the trustee, the protector, if any, the beneficiaries or class of persons or any other natural person exercising ultimate control over the *property* of the trust. It is not entirely in line with the standard which states that the beneficial owner shall be any natural person exercising ultimate effective control over the trust without limiting this to its property; although it may be inferred that effective control of the trust's property would in reality come down to the same thing.

120. *Criterion 10.12* - With regard to life insurance or investment related insurance business, Art. 19 (3) APMLFT requires FIs to conduct CDD on specifically named persons as soon as they are identified or designated and in cases where the beneficiary is designated by characteristics, class or other means they must satisfy themselves that they will be able to identify the beneficiary at the time of payment. Art. 19 (4) also requires the verification of identity at the time of payment**.**

121. *Criterion 10.13* - There are no requirements for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

122. *Criterion 10.14) -* Art. 19 APMLFT requires FIs to perform CDD measures *before* establishing a business relationship. Art. 21 adds that, where it is not possible to apply the measures referred to Art. 16 ((1) points 1, 2 and 3), the financial institution shall not establish a business relationship or effect a transaction. However, the Art. 19(2) suggests that there is also the possibility of delaying the application of CDD measures (including establishing the customer's identity) until some later (unspecified) point if this is necessary to preserve "uninterrupted normal conduct" (but only when there is little risk of ML/FT). The authorities have explained that Art. 19(2) does not determine the timeframe for any such delay, and that this depends on the particular obliged entity and its internal rules. Accordingly, evaluators consider that: (i) there is conflict between Art. 19(2) and Art. 21; and (ii) that the scope of the delay (which covers CDD measures referred to in points 1 and 2 of paragraph 1 of Art. 16) is wider that that permitted under this criterion (which is limited to verification of identity only).

123. *Criterion 10.15 -* FIs are not required to adopt risk management procedures under which the customer can utilise the business relationship prior to verification. However, as described under c.10.14, it is unclear whether there is a possibility for the customer to utilise the business relationship prior to completion of CDD.

124. *Criterion 10.16* - The APMLFT does not contain an explicit requirement to conduct CDD for existing customers. Such a requirement did exist under the old law (in force from 2007-2016, old

Art. 101) as far as high-risk customers were concerned. The legal CDD requirements have not changed substantially from the old to the new law (except for broadening definitions of BO and PEPs). Art. 16 and 49 require regular monitoring of business activities and verifying and updating of data and documentation for all customers depending on the risk level of the customer, commensurate to the ML/FT risk profile and at least 5 years since the last CDD.

125. *Criterion 10.17* - Art. 27 (1) point 6, Art. 43 (6), Art. 50, Art. 59, 60, 61 and 62 APMLFT specify the cases where additional due diligence measures are required in addition to the regular CDD obligations (when a customer is not physically present at the verification of his identity; if the data on the beneficial owner is obtained directly from the written statement of a statutory representative or his/her authorised person or only from the beneficial ownership register to be set up; if an unusual transaction presents an increased risk of ML or FT; entering into a correspondent banking relationship with a respondent bank or similar credit institution located in a third country; entering into a business relationship or carrying out a transaction with a customer who is a politically exposed person; when beneficiaries of life insurance or unit-linked life insurance and beneficial owners of the beneficiary are politically exposed persons; when a customer or transaction is linked with a high-risk third country. However this is not a closed list and in the second paragraph of Art. 59 the financial institution is required to identify further cases, on a risk based approach, where enhanced due diligence is required.

126. *Criterion 10.18* - Art. 57 APMLFT permits FIs to conduct simplified CDD in a manner specified in Art. 58 where the customer, business relationship, transaction, product, service, distribution channel, country of geographic area presents little risk so long as there are no reasons for suspicion of ML or FT regarding the customer, transaction, property or assets. The main difference with regular CDD lies in the scope of data on the customer and on the purpose and foreseen nature of the business relationship or translation that the financial institution must process.

127. *Criterion 10.19* - Art. 21 APMLFT sets out the requirement that if a financial institution cannot meet the CDD obligations in Art. 16 they should not establish a business relationship or effect a transaction or shall terminate the business relationship if it already exists. In addition, they should consider reporting data on the customer or suspicious transaction to the FIU.

128. *Criterion 10.20* - There is no provision in the law that allows FIs not to pursue CDD requirements where they suspect ML or FT and reasonably believe that performing the CDD process will tip off the customer.

Weighting and conclusion

129. Slovenia meets or mostly meets the vast majority of the criteria and the criteria that are partly or not met are relatively minor, with the exception of the lack of identification of beneficial owners of natural persons. There are clear requirements for FIs to undertake CDD measures with exception of wire transfers above EUR 1,000, where the requirement does not include the full range of CDD measures (e.g. identifying and verifying the beneficial owner). However since most wire transfers are carried out by banks with respect to existing clients, the evaluation team considers this deficiency as minor. For these reasons **Slovenia is LC with R.10.**

Recommendation 11 – Record-keeping

130. Slovenia was rated as largely compliant in the 4th round MER. There was no provision that would specifically require FIs to maintain records on account files and business correspondence. It was also established that no provision existed on maintaining CDD data and transaction records longer than five years if requested by competent authorities. The applicable law has changed, so the new analysis has been undertaken.

131. *Criterion 11.1* - FIs are obliged to maintain records on transactions for ten years after the termination of a business relationship, the completion of a transaction unless a longer period for retention is determined by another act (Art. 129 (1) APMLFT). The requirement covers both domestic and international transactions although APMLFT does not specifically distinguish between

them. Equally, EU Regulation 1781/2006 requires payment service providers to keep records of payer information for 5 years (Art. 11).

132. *Criterion 11.2* - FIs are required to keep all records obtained through CDD measures, account files and business correspondence and results of any analysis undertaken for ten years after the termination of a business relationship, the completion of a transaction, unless a longer period for retention is determined by another act (Art. 129 (1) and (2) APMLFT). Records that must be retained include the identification data of customers, their representatives and authorized persons, date of establishing the business relationship, its purpose and intended nature, business operations and origin of assets used, as well as the analysis of background and purpose of unusual transactions, and grounds of ML/FT suspicions. APMLFT addresses the shortcoming identified in the previous MER by specifically requiring FIs to keep "copies or records or originals of the documentation on business relationships and account files" (Art. 129 (2)).

133. *Criterion 11.3* - APMLFT requires FIs to keep the necessary elements of transaction records that should be sufficient to permit reconstruction of individual transactions (Points 6 to 9 of Art. 137(a)). Moreover, Art. 8 of the Rules on Performing Internal Control, Authorized Person, Safekeeping and Protection of Data and Keeping of Records of Organizations, Lawyers, Law Firms and Notaries provides for the requirement to maintain data in such a manner as to permit reconstruction of individual transactions: "The obliged person shall keep the data and the corresponding documentation relating to the implementation of the Act in a chronological order and in a manner that enables access in an entire period, as is the safekeeping thereof prescribed in accordance with the Act."

134. *Criterion 11.4* - Art. 91 and Art. 115 APMLFT explicitly permit OMLP to access CDD data and transaction records held by FIs (see the analysis for c. 9.1). In case of ML/FT suspicion, such data and records must be provided to OMLP within 15 days from the request, or in a shorter time limit set by OMLP in urgent cases. OMLP is also authorized to request and be provided, without delay and at the latest within eight days of receiving the request, with any information from FIs that is needed for supervisory purposes (Art. 141). Other supervisors have the power to obtain necessary AML/CFT information and documents from FIs based on sector-specific legislation. The authorities confirmed that the deadline for submitting the requested information is usually determined by the competent supervisory authority, having taken into account the extent of the requested data. For instance, Art. 241 BA stipulates that a bank should submit all requested data and information in a way and form, determined by BoS, within a time-frame set by BoS, but not shorter than three days from the receipt. As for LEAs, CPC allows the investigating judge to require banks, savings banks or savings-credit services to disclose information based on grounded request of the public prosecutor (Art. 156).

135. *Weighting and Conclusion*: All of the 4 criteria are met. **Slovenia is compliant (C) with R.11.**

Recommendation 12 – Politically exposed persons

136. Slovenia was rated as largely compliant in the 4th round MER. The definition of politically exposed persons (PEPs) was not sufficiently broad to include all categories of natural persons performing a prominent public function. No clear requirements existed in relation to customers that become PEPs during the business relationship. FIs were not required to determine whether the customer's beneficial owner was a PEP. The FATF standards in this area were revised since then and the applicable law has changed, so the new analysis has been undertaken.

137. *Criterion 12.1* - The definition of foreign PEPs is provided by Art. 61 of APMLFT and includes natural persons who are or have been entrusted with a prominent public function in a Member State or third country within the previous year, including their immediate family members and close associates, namely:

(i) heads of state, prime ministers, ministers and their deputies or assistants;

(ii) elected representatives in legislative bodies;

(iii) members of management bodies of political parties;

(iv) members of supreme and constitutional courts, and other high-level judicial authorities against whose decisions there is no ordinary or extraordinary legal remedy save in exceptional cases;

(v) members of courts of audit and boards of governors of central banks;

(vi) heads of diplomatic missions and consulates, and representations of international organisations, their deputies and high-ranking officers of armed forces;

(vii) members of the management or supervisory bodies of undertakings in majority state ownership;

(viii) representatives of bodies of international organisations (such as presidents, secretaries-general, directors, judges), their deputies and members of management bodies or holders of equivalent functions in international organisations.

(a) APMLFT imposes an explicit obligation on FIs to put in place risk management systems for identifying PEPs, and extends this requirement to the beneficial owner of a customer (Art. 61(1)).

(b) APMLFT requires an employee of the FI establishing a business relationship with a PEP to obtain a written approval of a superior responsible person from senior management (Point 2 of Art. 61(6)). It is not clear to what extent this requirement applies in situations when a customer or a beneficial owner becomes a PEP after the establishment of the business relationship.

(c) APMLFT requires FIs to obtain data on the customer's "wealth", and on the "source of funds and property" that are, or will be, the subject of the business relationship or a transaction (Point 1 of Art. 61(6)). Authorities claimed that the term "wealth" should be interpreted widely so as to also include its sources. FIs are not required to take reasonable measures to establish either the source of wealth or the source of funds of the beneficial owner identified as a PEP.

(d) FIs must monitor the business relationships with PEPs with "special due diligence" (Point 3 of Art. 61(6)). Authorities explained that the term "special" amounts to "enhanced" and would normally require increasing the number and timing of controls applied by FIs.

138. *Criterion 12.2* - APMLFT extends the definition of a PEP to all natural persons entrusted with a prominent public function in EU member states or third countries (Art. 61(2)). The representatives of bodies of international organisations (such as presidents, secretaries-general, directors and judges), their deputies and members of management bodies or holders of equivalent functions in international organisations are also part of the list of natural persons performing a prominent public function (Art. 61(3)). Thus, both domestic PEPs and natural persons entrusted with a prominent function in an international organisation are subject to the same CDD measures as foreign PEPs. However, this Criterion is affected by deficiencies identified under c. 12.1.

139. *Criterion 12.3* - Immediate family members and close associates are subject to the same CDD measures as all other types of PEPs. The new APMLFT established a more comprehensive definition of close associates, which covers joint beneficial ownership of legal entities or legal arrangements, or any other close business relationships with PEPs (Art. 61(5)). A natural person who has the sole beneficial ownership of a legal entity or legal arrangement that is known to have been set up for the benefit of a PEP is also considered as a close associate. However, this Criterion is affected by deficiencies identified under c. 12.1.

140. *Criterion 12.4* - FIs are required to set up adequate measures to establish, whether beneficiaries of life insurance and other investment-related insurance policies or their beneficial owners are PEPs. These measures shall be adopted at the latest at the time of the pay out or in the case of an assignment, in whole or in part, at the time of the assignment. If higher risks are established, FIs shall take additional measures, which include informing a superior responsible person from senior management before the pay out, conducting special (enhanced) scrutiny of the business relationship with the policyholder, and in case of suspicion of ML/FT, reporting to the OMLP (Art. 62 of APMLFT).

Weighting and Conclusion

141. The shortcomings related to c.12.1 include the absence of the clear requirement to take reasonable measures for establishing the source of wealth of customers that are identified as PEPs. There is also no requirement to take reasonable measures to ascertain the sources of wealth and funds of the beneficial owner identified as a PEP. Moreover, it is also not entirely clear to what extent the requirement to obtain a senior management approval applies to an existing customer or beneficial owner that becomes a PEP. These shortcomings also affect c. 12.2 and 12.3, and underpin the overall rating. **Slovenia is PC with R.12.**

Recommendation 13 – Correspondent banking

142. Slovenia was rated as largely compliant in the 3rd round MER, but was not evaluated with the previous R.7 in its 4th round assessment. The 3rd round MER noted that the same requirements applied to relationships with foreign banks as to any other foreign legal persons. Since the FATF standards in this area were revised and the applicable law has changed, a new analysis has been undertaken.

143. *Criterion 13.1* - Application of additional measures provided by Art. 60 APMLFT is limited to only cross-border correspondent relationships with credit institutions from non-EU member countries, which is not in line with the FATF standards.

(a) According to the APMLFT, FIs are required to apply CDD measures with respect to potential respondent institutions, including by obtaining data on the purpose and intended nature of the business relationship (Art. 60 (1)). However, there is no explicit requirement to understand the nature of the respondent's business.

In addition, the establishment of a cross-border correspondent relationship is allowed after obtaining information about AML/CFT systemic arrangements in a country where the respondent institution is registered or established (Point 3 of Art. 60 (1)). The APMLFT also requires the written statement from a respondent institution that it is subject to the administrative supervision and falls under the obligation to comply with applicable AML/CFT laws and regulations (Point 6 of Art. 60 (1)). However, these measures do not amount to determining the reputation of an institution or the quality of supervision, including whether it has been subject to ML/FT investigations or regulatory actions.

(b) With regard to the assessment of the respondent institution's AML/CFT controls, the APMLFT only requires obtaining description of the performance of internal procedures relating to the detection and prevention of ML/FT (Point 2 of Art. 60 (1)).

(c) An employee establishing a cross-border correspondent relationship must obtain a written approval of a "superior responsible person" from senior management prior to entering into a relationship (Art. 60 (2)).

(d) There is no requirement to clearly understand the respective AML/CFT responsibilities of each institution.

144. *Criterion 13.2* - There are no specific requirements provided for by the AML/CFT legislation with respect to payable-through accounts.

145. *Criterion 13.3* - APMLFT prohibits entering into or continuing a correspondent relationship with shell banks or other institutions that are known to allow shell banks to use their accounts. This obligation applies to all respondent institutions no matter where they are located (Art. 66 of APMLFT). In addition to that, the APMLFT imposes an obligation to obtain a written declaration from respondent banks that they do not operate as a shell, and have no established relationship with shell banks. However this written statement is mandatory only in the case of establishing a correspondent relationship with a bank situated in a third country (Art. 60, par. 5 and 5). The AML/CFT guidelines issued by the BoS explain that this type of statement is not expected from banks with a registered office in EU Member States or those situated in equivalent third countries. No such statement is also

required from a bank with a registered office in the EU or an equivalent third country, but under the majority ownership of a bank with a registered office in a third country (Sect. 2.6.2).

146. APMLFT defines the shell bank as a financial institution registered in a jurisdiction in which it does not perform its activities and which is not affiliated with a supervised or otherwise regulated financial group (Art. 3 (27)). However, APMLFT does not say that an FI must also be subject to an "effective" supervision in order to not be considered as a shell bank as required by the FATF standards.

Weighting and Conclusion

147. The deficiencies in c.13.1 include the application of additional measures provided by APMLFT only to institutions from non-EU member countries. In addition, there is no explicit requirement for FIs to understand the nature of the respondent's business. FIs are also not required to clearly understand the responsibilities of each institution, and to conduct the assessment of a respondent institution's AML/CFT controls. The additional measures provided by APMLFT are insufficient to require FIs to determine the reputation of a respondent or the quality of supervision applied to it. There are no measures in place to address the requirements of c. 13.2. In relation to c. 13.3, the definition of a shell bank is not fully in line with the FATF standards. **Slovenia is PC with R.13.**

Recommendation 14 – Money or value transfer services

148. Slovenia was rated as compliant in the 4th round MER. Since the FATF standards in this area were revised and the applicable law has changed, the new analysis has been undertaken.

149. *Criterion 14.1* - The PSSA allows banks, electronic money undertakings and payment institutions to perform payment services based on the authorization of the BoS (Art. 17 PSSA). The Act also permits the establishment of waived payment institutions to perform limited money remittances. The BoS can waive some of the authorization requirements related to the legal form of organization or the governance and internal control systems for waived institutions (Art. 67 PSSA). Although, EU legislation allows EU-based payment institutions to operate in Slovenia without acquiring separate license, BoS must be notified by the home country supervisor based on Art. 43 PSSA. Every entity that intends to perform payment services is required to provide the BoS with the description of internal control mechanisms for ensuring compliance with AML/CFT requirements (Art. 29 and 43 PSSA).

150. *Criterion 14.2* - Art. 201 PSSA authorizes BoS to verify whether a natural or legal person is providing payment services without authorization by examining relevant business books and other documents. If the conduct of unauthorized payment services is confirmed, BoS can issue a cease and desist order or issue a fine of 2.500 EUR to 80.000 EUR (Art. 230 PSSA). It may also request the court to initiate the liquidation proceedings when the cease and desist order is not complied with (Art. 203 PSSA).

151. *Criterion 14.3* - According to PSSA, MVTS are included in the definition of payment services, which are only allowed to be provided by Payment service providers (PSPs) (Art. 5 and 17). PSPs are designated as obliged entities and are subject to AML/CFT supervision by OMLP and BoS under the APMLFT (Art. 4 (1) and 151 (1) respectively). This includes PSPs from other EU Member States that do not need a license in Slovenia and are being supervised by BoS in cooperation with the home country supervisor.

152. *Criterion 14.4* - Agents of PSPs are not required to be licensed or registered by a competent authority. However, every agent operating in Slovenia or a third country must be included in the centralized register of PSPs[75] maintained by BoS under Art. 69 of the Payment Services and Systems

[75] www.bsi.si/en/payment-systems.asp?MapaId=1487

Act. The register is public and free-of-charge, and includes names and addresses of individual agents, as well as the information about specific MVTS provided. BoS makes sure that the register is regularly updated and removes an agent from the register once the provision of payment services through an individual agent is terminated (Art. 73).

153. *Criterion 14.5* - The PSSA stipulates that PSPs are fully responsible for the compliance of their agents with applicable legal requirements (Art. 39). Thus, PSPs are required to also apply appropriate AML/CFT controls as provided by APMLFT and relevant regulations to individual agents. Moreover, notifications to BoS on the intention to perform payment services through an agent must be accompanied with the description of internal controls that will be used by agents in order to comply with AML/CFT requirements (Art. 36 PSSA).

Weighting and Conclusion

154. All of the 5 criteria are met. **Slovenia is C with R.14.**

Recommendation 15 – New technologies

155. Slovenia was rated as partially compliant in the 4th round MER. There was no specific requirement in the legislation that would require FIs to have policies in place or take such measures as may be needed to prevent the misuse of technological developments. FATF standards were revised since then by incorporating requirements on a non-face to face business in R.10, and putting more emphasis on the identification and mitigation of risks arising from new products and technologies in R.15. The applicable law has also changed and the new analysis was undertaken.

156. *Criterion 15.1* - APMLFT requires FIs to analyse the impact of all major changes in business processes, including the introduction of new products and technologies, on their ML/FT risk exposure (Art. 13 (6) APMLFT). The Bank of Slovenia Regulation on Internal Governance Arrangements, the Management body and the Internal Capital Adequacy Assessment Process for Banks and Savings Banks also requires banks to assess risks of any significant changes in existing products or in introduction of new services and systems (Art. 27, 28 and 30). Although the regulation targets the general risk management procedure, according to Slovenian authorities, it is also applicable for AML/CFT purposes.

157. AML/CFT guidelines issued by BoS explain in detail the ML/FT risk analysis that must be performed by banks in relation to all products and services. The guidelines also require banks to establish a procedure for regular update of the existing risk analysis based on the assessment of new risks resulting from changes in the manner of operations, including the introduction of new services (Sect. 3). Similarly, guidelines issued by ISA (Sect. 9) and SMA (Sect. 11) provide detailed guidance on the analysis of ML/FT risks and require assessment of the impact of all significant changes in business processes, such as introduction of new products and technologies, on an institution's ML/FT risk exposure.

158. *Criterion 15.2* - The requirement to carry out risk assessment prior to launching or using new products, practices and technologies is clearly provided under Art. 13 (7) APMLFT. It is further affirmed by the Bank of Slovenia Regulation on Internal Governance Arrangements, the Management body and the Internal Capital Adequacy Assessment Process for Banks and Savings Banks, which stipulates that new products and services can only be approved based on the results of risk assessments (Art. 30). AML/CFT guidelines issued by ISA (Sect. 9) and SMA (Sect. 11) follow the wording used in Art. 13 (6) APMLFT and require introduction of new products and technologies to be analysed relative to their impact on an institution's risk exposure.

159. APMLFT specifically provides for the adoption of appropriate measures to reduce ML/FT risks identified through the impact assessment of new products and technologies (Art. 13 (7)). The Bank of Slovenia Regulation on Internal Governance Arrangements, the Management body and the Internal Capital Adequacy Assessment Process for Banks and Savings Banks says that unless adequate risk management processes are put in place banks are not permitted to launch new products (Art. 30). AML/CFT guidelines issued by the Bank of Slovenia (Sect. 5.4), the Insurance

Supervisory Agency (Sect. 8 and 9) and the Securities Market Agency (Sect. 11) require application of appropriate policies, procedures and controls before new products and services are launched or existing ones are modified in such a way as to pose ML/FT risks.

Weighting and Conclusion

160. Both criteria are met. **Slovenia is C with R.15.**

Recommendation 16 – Wire transfers

161. Slovenia was rated as compliant with the previous SR.VII. However, FATF standards in this area have been significantly revised. APMLFT contains no provisions in relation to wire transfers – since the EU Regulation 1781/2006 applies directly in all EU members states, including Slovenia. At the national level, BoS issued AML/CFT guidelines for the banking sector that provide for recommendations to meet the requirements of the EU Regulation. A successor EU Regulation 2015/847 was adopted in 2015, but will only come into force from 26 June 2017 and thus will not be taken into account in this analysis.

Ordering FIs

162. *Criterion 16.1)* - FIs are required to make sure that all cross-border wire transfers exceeding EUR 1,000 are accompanied with the complete and verified information about the payer under the EU Regulation (Art. 4 and 5 EU Regulation 1781/2006). However, there is no requirement for ordering FIs to also provide the beneficiary information in the case of cross-border transfers.

163. *Criterion 16.2* - The EU Regulation does not require complete information about the payer to accompany each individual transfer in case of batch files from a single payer, when PSP of the payee is situated outside the European Economic Area (EEA). Nevertheless, batch files should contain the complete payer information, while individual transfers must be carrying the payer's account number or unique identifier (Art. 7(2) EU Regulation 1781/2006). There are no such requirements in relation to the beneficiary information.

164. *Criterion 16.3* - All cross-border wire transfers must be accompanied with the complete information about the payer regardless of the amount of funds under the EU Regulation (Art. 4 and 5). However, there is no requirement for FIs to ensure that such transfers also include the beneficiary information.

165. *Criterion 16.4* - Information about the payer may not be verified for cross-border wire transfers under EUR 1 000 according to Art. 5(4) of the EU Regulation. However, the same provision states that this can only be done without prejudice to the Third Money Laundering Directive (2005/60), which requires application of full CDD measures in case of ML/FT suspicion (Art. 7 (c)). APMLFT also provides for CDD measures whenever there is a suspicion of ML/FT offence, regardless of the amount of funds (Art. 17(1).

166. *Criteria 16.5 & 16.6* - The EU Regulation treats wire transfers where both the payer and the payee PSPs are situated within the EEA as domestic transfers, which is in line with the FATF standards. Such transfers of funds can be accompanied only by the payer's account number or unique identifier that allows the transaction to be traced back to the payer provided that the complete payer information will be made available within three working days upon the request from the payee's PSP (Art. 6 EU Regulation 1781/2006). APMLFT ensures that competent authorities have access to the customer identification data and transaction records (see the analysis for Criterion 9.1).

167. *Criterion 16.7* - Ordering FIs are required to keep records of all the information about the payer for 5 years under the EU Regulation (Art. 5(5)). However, there is no obligation to keep the beneficiary information. APMLFT provides for the general requirement to retain "the personal name and permanent address or name and registered office of the person to whom the transaction is directed" for ten years when the transaction amounts to 1,000 or more (Art. 58 (5.2)).

168. *Criterion 16.8* - Ordering FIs must comply with the requirements of the EU Regulation on the information about the payer before executing wire transfers. At the domestic level, the Government

Decree on the Implementation of the EU Regulation lays down penalties for ordering PSPs when they fail to ensure that transfers are accompanied with the complete payer information (Art. 4(1)). However, FIs are not required to consider the absence of the beneficiary information as a ground for refusing transfers of funds.

Intermediary FIs

169. *Criterion 16.9* - The EU Regulation requires intermediary PSPs to make sure that all information received on the payer is kept with the transfer of funds (Art. 12). However, there is no such requirement in relation to the beneficiary information.

170. *Criterion 16.10* - Intermediary PSPs are permitted by the EU Regulation to use a payment system with technical limitations provided that they make all the payer information received available to the beneficiary FIs upon request and within three working days (Art. 13(4)). Intermediary PSPs are also required to keep records of the payer information they are provided with for 5 years. However, these requirements do not extend to the beneficiary information.

171. *Criterion 16.11* - Intermediary FIs are not required to take reasonable measures to identify cross-border transfers of funds that lack originator or beneficiary information.

172. *Criterion 16.12* - Intermediary FIs are not required to have risk-based policies on responding to the missing originator or beneficiary information and taking appropriate follow-up actions.

Beneficiary FIs

173. *Criterion 16.13* - The EU Regulation requires beneficiary FIs to have effective procedures in place to identify whether the payer information is missing (Art. 8). The Bank of Slovenia AML/CFT guidelines provide for detailed recommendations on detecting the missing payer data during the processing of payment orders or through post-event random sampling (Sect. 4.3). However, there is no obligation to detect the missing beneficiary information.

174. *Criterion 16.14* - Beneficiary FIs are not required to verify the identity of the beneficiary if it was not previously verified for transfers of EUR 1,000 or more. APMLFT contains the general requirement for FIs to identify and verify the customer's identity when carrying out an occasional transaction of EUR 15,000 or more (Art. 17(2)). The record-keeping requirements provided by APMLFT apply once the information and documents for verification purposes are obtained (Art. 129 and 137).

175. *Criterion 16.15* - When information on the payer is missing or incomplete, beneficiary FIs are required to reject the wire transfer or ask for complete information in accordance with the EU Regulation (Art. 9(1) EU Regulation 1781/2006). However, there is no provision for the suspension of transfers pending receipt of the complete payer information. The Bank of Slovenia AML/CFT guidelines also conclude that "no legal basis exists to hold funds on the grounds of incomplete information regarding a payer" when requesting the missing information. Furthermore, the guidelines note that a common decision was taken by Slovenian banks to not automatically reject payment orders with incomplete information about the payer, but instead attempt to obtain the missing data. Therefore, the Bank of Slovenia recommends banks to execute payment orders and take appropriate steps to obtain the missing payer information (Sect. 4.4).

176. The EU Regulation requires beneficiary FIs to consider missing or incomplete payer information as a factor in determining whether a transfer of funds is suspicious and must be reported to competent authorities (Art. 10 EU Regulation 1781/2006). Where the originating FI regularly fails to provide complete information on the payer, a beneficiary FI is required to consider rejecting all future transfers or terminating the business relationship after issuing warnings and setting deadlines, and to report the fact to competent authorities (Art. 9(2) EU Regulation 1781/2006). The Bank of Slovenia AML/CFT guidelines define the regular failure in providing complete information on the payer by laying down specific criteria (Sect. 4.7). All of the above requirements do not extend to instances when the beneficiary information is missing.

Money or Value Transfer Service Operators

177. *Criterion 16.16* - The EU Regulation applies to all PSPs, which are defined as natural or legal persons whose business includes the provision of transfer of funds (Art. 2(5)). However, absence of requirements related to the beneficiary information indirectly affects this criterion.

178. *Criterion 16.17* - The EU Regulation does not specifically require PSPs controlling both the ordering and beneficiary side of a transfer to consider all the information from both sides when deciding whether to file an STR. APMLFT provides for general obligations of payment service providers to identify and report suspicious transactions.

Implementation of Targeted Financial Sanctions

179. *Criterion 16.18* - FIs conducting wire transfers are subject to EU regulations that give effect to UNSCRs 1267, 1373, and successor resolutions. However, gaps identified under Criterion 6.4 could adversely affect the ability of FIs to implement targeted financial sanctions in a timely fashion.

Weighting and Conclusion

180. The absence of requirements in relation to beneficiary information is the main deficiency for criteria 16.1, 16.2, 16.3, 16.7, 16.8, 16.9, 16.10, 16.13 and 16.15, which also indirectly affects c.16.6. Another serious problem is the lack of the requirement for intermediary FIs to identify missing originator or beneficiary information and apply risk-based policies (c.16.11 and 16.12). **Slovenia is PC with R.16.**

Recommendation 17 – Reliance on third parties

181. Slovenia was rated as compliant in the 3rd round MER and was not evaluated with the previous R.9 in its 4th round assessment. The FATF standards in this area were revised since then to stress the importance of a third party country risk.

182. *Criterion 17.1* - APMLFT permits reliance on certain types of FIs and DNFBPs to perform CDD measures except for the ongoing monitoring of the business relationship. However, ultimate responsibility for the proper application of CDD measures rests with relying FIs (Art. 51 (4) APMLFT).

(a) & (b) - APMLFT requires that a third party must make the CDD data available to a relying institution immediately, and also provide copies of documents related to CDD immediately upon request (Art. 54 (1)-(3)). FIs must make sure in advance that third parties can meet these requirements (Art. 51(2)). FIs are prohibited from establishing the business relationship with a customer if the third party fails to provide the CDD data in advance (Art 54(5)).

(c) - APMLFT does not require FIs to make sure that *all* third parties are regulated, and supervised or monitored for, and have measures in place for compliance with the relevant CDD and record-keeping requirements. APMLFT provide for a number of groups of FIs and DNFBPs that could be relied upon as third parties (Art. 52). The first group consists of those institutions that are regulated and supervised for AML/CFT purposes by Slovenian authorities, and are required to apply CDD and record-keeping measures under APMLFT. The second group includes entities based in third countries provided that they are required to comply with equal or equivalent CDD and record-keeping provisions, and are being supervised with equal or equivalent provisions as laid down in APMLFT. However, no such requirements apply to the third group, which is comprised of certain institutions and their branches established in EU Member States, including branches of investment fund management companies from third countries, and consular offices of the Republic of Slovenia in other EU Member States and third countries.

183. *Criterion 17.2* - APMLFT prohibits reliance on third parties that are established in third countries listed as high-risk (Art. 52 (7)). However, the third party reliance is permitted in case of EU Member States without having regard to the information about the level of country risk. Apparently, it is presumed that all EU members universally apply appropriate AML/CFT standards without the need to conduct individual country risk assessments, which falls short of the c.17.2. APMLFT also

allows FIs to entrust CDD measures to third parties established in high-risk third countries or countries with higher probability of ML/FT occurrence provided that they are branches or majority-owned subsidiaries of institutions which are based in EU Member States (Art. 52(8)).

184. *Criterion 17.3* - Within the scope of group policies, FIs may entrust the application of CDD measures to a third party which is a member of the group provided:

(a) the group applies CDD and record-keeping measures, and has appropriate AML/CFT programs in place that are equal or equivalent to the provisions of the APMLFT;

(b) the implementation of CDD and record-keeping obligations at the group level is supervised by Slovenia's relevant supervisory authority or the competent authority of a Member State or a third country.

(c) However, there is no specific requirement for any higher country risk to be adequately mitigated by the group's AML/CFT policies.

Weighting and Conclusion

185. The shortcomings in c.17.1 include the lack of requirement for FIs to satisfy themselves that third parties established in EU Member States are regulated, and supervised or monitored for, and have measures in place for compliance with appropriate CDD and record-keeping obligations. In relation to c.17.2, permitting reliance on EU-based FIs or their branches and majority-owned subsidiaries in third countries as third parties on the basis of the presumption that all EU-based FIs would ensure application of appropriate AML/CFT measures is the deficiency. Lastly, there is no specific requirement to adequately mitigate the higher country risk at the group level, which contradicts the c.17.3. **Slovenia is LC with R.17**.

Recommendation 18 – Internal controls and foreign branches and subsidiaries

186. In its 4th round MER Slovenia was found to be largely compliant with former R. 15 and R. 22. Weaknesses identified were lack of specific employee screening provisions, a need to clarify compliance officer requirements, and the requirement to observe AML/FT measures in branches and subsidiaries is limited to those located in third countries. The applicable law has changed, so the new analysis has been undertaken.

187. *Criterion 18.1* - To carry out efficient mitigation and management of risk of ML/FT, the obliged person shall establish efficient policies, controls and procedures that are proportional in terms of his/her activity and size. (Art 15 (1) and (2) APMLFT).

(a) The obligation to appoint an AML/CFT compliance officer (referred to as an "authorised person") at management level is met by the requirement set out in Art. 76 and 77 APMLFT. Art. 77 states that such a person must hold a position that is high enough in rank to enable the rapid, quality and timely execution of tasks. Obliged entities, which are a medium or large companies, are also obliged to appoint one of the members of the management board or management authority to be responsible for establishing policies, controls and procedures and for ensuring the compliance of implementation of acts and other regulations from the field of detection and prevention of ML/FT (Art 15 (3) APMLFT). Prior to introducing policies, controls and procedures, obliged persons shall acquire the approval of the management, and according to the guidelines of supervisory bodies monitor and, if required, strengthen the measures adopted (Art 15(4) APMLFT).

(b) Policies, controls and procedures shall also cover secure employment (though it is not explained what this term means nor who should be covered) and, if required, security clearance of employees governing classified information. (Art 15 (1) and (2) APMLFT). The authorities consider that this provision covers all employees. Conditions for suitability of AML/CFT compliance officers are defined in Art. 77 APMLFT.

(c) It is not specified that policies, controls and procedures should cover training. Instead, there is an obligation to provide regular AML/CFT training of employees under Art. 80 APMLFT. This provision requires an annual training programme to be drawn up.

(d) Policies, controls and procedures shall also cover establishment of an independent internal audit department to verify internal policies, controls and procedures if the obliged person is a medium-sized or large company as per the Act governing companies (Art. 15 (1) and (2) APMLFT). Art. 141 and 142 BA also regulate the appointment and the responsibilities of the audit function in banks and these are developed in more detail in relation to AML/CTF in section 1 of the Bank of Slovenia guidance.

188. *Criterion 18.2* - A general obligation to implement group AML/CFT policies and procedures to branches and subsidiaries in which the obliged person has a controlling interest is established in Art. 71(2) APMLFT. Further explanation as to the implementation of group policies and procedures has still to be defined in sector specific guidance.

(a) Art. 71(1) APMLFT stipulates that obliged entities that are a part of a group shall implement the policies and procedures of the group that relate to measures for detecting and preventing ML/FT, including, amongst other things, policies and procedures regarding information exchange within the group for the purposes of preventing ML/FT. Legislation further provides that exchange of information by an obliged person inside its group is allowed, including the exchange of information on suspicious transactions, unless the OMLP explicitly opposes the exchange of information on suspicious transactions (Art. 71 (3) APMLFT).

(b) The law requires the implementation of policies and procedures of a group and measures for detecting and preventing ML/FT in branches and majority-owned subsidiaries located in third countries (Art. 12 (2, point 9)), though there is no provision for branches and subsidiaries in EU countries as the term “third countries” within the APMLFT does not include the EU.

Art. 75(1) also requires obliged entities to ensure that the measures for detecting and preventing ML/FT as stipulated in this Act are also implemented at equal or higher level in its branches and its majority-owned subsidiaries established in 'third countries'.

(c) Before transmission of data to third countries the law requires an obliged entity to obtain the written guarantee of the intended recipient of data that: (i) it ensures the same level of personal data protection as the obliged entity; and (ii) the third country guarantees the appropriate level of personal data protection (Art 71 (4) APMLFT). Art. 123 (regarding data disclosure) also permits disclosure of data with group entities, provided that group AML/CFT policies and procedures and personal data protection are in line with Slovenian requirements. However, these provisions regulate the sharing of information by the obliged person with its group, and not also the sharing of information by branches and subsidiaries, outside Member States, with the obliged person.

189. *Criterion 18.3* - Art. 75(1) APMLFT stipulates a general and overall provision for obliged entities to ensure measures for ML/FT prevention and detection are applied in majority-owned subsidiaries and branches at least to the same extent as stipulated in the APMLFT, where accommodated in the law of the third country (countries outside of EU). Art. 75 (2) APMLFT stipulates that, if the minimum standards of implementing the measures for detecting and preventing ML or FT in third countries are less strict than the measures prescribed in the APMLFT, the obliged person shall ensure that its branches or its majority-owned subsidiaries adopt and implement suitable measures equivalent to the measures prescribed in APMLFT, within the laws of the respective third country. Suitable measures also include measures for data protection. If the law of a third country does not allow implementation of such suitable measures (or AML/CFT policies and procedures), an obliged person shall provide that branches and majority-owned subsidiaries in the third country adopt and implement suitable additional measures through which they manage risks of ML and FT and notify the competent supervisory authorities (Art 75 (4) APMLFT). The Bank of Slovenia, Securities Market Agency and Insurance Supervision Agency shall notify European

supervisory bodies and competent supervisory bodies of other Member States of this, namely for the purpose of harmonising activities in finding a suitable solution (Art 75 (3) APMLFT).

Weighting and conclusion

There are deficiencies with respect to reporting entities' internal controls. However, since only one bank in Slovenia has foreign branches, the evaluation team does not deem the deficiencies under c. 18.2 (rated with partly met) to be very serious in the context of Slovenia. **Slovenia is LC with R.18.**

Recommendation 19 – Higher-risk countries

190. In the 4th round evaluation Slovenia was rated compliant with the previous R.21. The new R.19 contains new requirements that were not assessed under the previous methodology.

191. *Criterion 19.1* - Article 59(1) para 4) Art. 59(1) APMLFT requires an obliged person to apply enhanced due diligence where a customer or transaction is linked to a high-risk *third country* (rather than all high risk countries). There is no explicit requirement in the law or other enforceable means to apply enhanced due diligence proportionate to the risks to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

192. *Criterion 19.2* - According to the second point of Art. 50(3), FIs shall exercise special care when dealing with unusual transactions (but not otherwise) of customers related to countries listed by the OMLP under Art. 50(6) - a list of countries with a "great possibility" of ML/FT. This may include countries subject to a call from the FATF or which have been identified by competent international organisations, e.g. MONEYVAL. Also, under Art. 68 APMLFT, FIs must submit to the OMLP data of every transaction that exceeds EUR 15 000 with a person from, or with an address in, a high risk country (listed in a delegate act or by the OMLP). The limitation of the "special care" provision only to unusual transactions does not enable the provision of a wide range of countermeasures that can be applied proportionately to risks.

193. *Criterion 19.3* - OMLP and BoS publish a list of countries where there are weaknesses in their AML/CFT system and update by email when necessary.

Weighting and Conclusion

194. Identified deficiencies are minor. There is no explicit requirement in the law or other enforceable means to apply enhanced due diligence proportionate to the risks to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF. The limitation of the "special care" provision only to unusual transactions does not enable the provision of a wide range of countermeasures that can be applied proportionately to risks. **Slovenia is rated LC with R 19**.

Recommendation 20 – Reporting of suspicious transaction

195. Slovenia was rated largely compliant during the 4th round with the former R. 13 and SR. IV. The main reasons for such rating were the concerns related to effectiveness - the low numbers of STRs from outside the banking sector and from the insurance companies. In relation to the FT reporting regime, it was noted by the assessors that only "property" linked with a transaction was covered by the reporting obligation.

196. *Criterion 20.1* - The obligation for FIs to submit a report where they suspect or have reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing is provided under Art. 69 APMLFT. Reporting entities are required to report a transaction to the OMLP (via a secure electronic channel) prior to executing it if there is suspicion that the transaction, person, property or assets are the proceeds of (or are involved in) money laundering, predicate offences or terrorist financing activities. Exceptionally, the reporting may be done by telephone (however, the reporting shall be made once again via a secure electronic channel the

working day at the latest) or in writing. If the obliged entity cannot act according to the prescribed procedure - due to the nature of transaction or if the transaction has not been performed at all or due to other justified reasons - such information shall be reported immediately to the OMLP (including the reasons). A STR shall be submitted even in the absence of transaction but with regard to clients having suspicious behaviour, for example. Although the APMLFT does not specifically refer to promptness of such reporting, whereas the assessment team deems that the explanations concerning the means to report the suspicious transaction (e.g. transaction reported over the phone needs to be done via secured channel next working day at the latest) fulfil this requirement.

197. *Criterion 20.2* - Art. 69(3) APMLFT imposes the reporting entities the obligation to report intended transaction, irrespective of whether this was made at a later date or not. No threshold is specified in the law, neither in the indicators provided by the OMLP. Nonetheless, in the absence of clear guidelines, it remains unclear to the evaluation team how the reporting entities shall establish the intent for executing transaction(s) since the wording ('intended') is rather considered as a mental element and does not directly cover the FATF standard which requires reporting of attempted transactions. The authorities advised that, in practice, the intention could only be demonstrated through the verbal or written order which had not been executed yet. Also any other information that can confirm an intention could be taken into account. Therefore, the assessment team deems that this requirement of the standard is covered.

Weighting and Conclusion

198. Both criteria are met. **Slovenia is C with R.20.**

Recommendation 21 – Tipping-off and confidentiality

199. Slovenia was not assessed in the 4th round against the requirements of former R. 14 but was rated Largely compliant on this recommendation in the 3rd round given that that the "safe harbour" provisions did not clearly cover criminal liability.

200. *Criterion 21.1* - Art. 126 (2) APMLFT exempts FIs and their staff from liability for the damage caused to customers or to third parties when submitting or obtaining data, information and documentation to the OMLP. Same applies for the implementation of an order to temporarily suspend or monitor a transaction of a customer. Additionally, par. 3 of the same article provides protection to the staff of FIs from criminal or disciplinary liability for breaching the obligation to protect classified data, business secrets, and confidential bank data, when, in line with the law, they submit them to OMLP for the purpose of verifying customers and transactions when there are grounds to suspect ML/FT. The law does not provide explicit protection in cases the reporting entity and its employees did not know the exact underlying criminal activity. Nevertheless, the protection covers all instances of sending data, information and documentation. Authorities advised that the STRs reporting obligation provided in Art. 69 APMLFT covered reporting of suspicious transactions regardless of the fact if the reporting entity knew the underlying criminal activity. Therefore, and for the reason of acting in line with the respective law, the obliged entities or their staff could not be held liable for possible damage. In the opinion of the assessment team these provisions sufficiently cover the FATF requirements with regard to c.21.1.

201. *Criterion 21.2* - The prohibition required by this criterion is introduced through Art. 122 APMLFT. The ban on disclosing the data shall not be in effect if this is a disclosure of data carried out among credit institutions and FIs from Member States which are a part of the same group, under the condition that the policies and procedures of the group are equal to the provisions of the APMLFT (Art. 123). Sanctions for cases of violation of the provisions of Art. 122 are set out in Art. 163 and 165 APMLFT.

Weighting and Conclusion

202. Both criteria are met. **Slovenia is C with R.21.**

Recommendation 22 – DNFBPs: Customer due diligence

203. Slovenia was rated as partially compliant in the 4th round MER. The weaknesses identified in relation to FIs also applied to DNFBPs. In addition, there was no clear requirement for real estate agents to carry out CDD measures with respect to both purchasers and vendors of the property, and a notable lack of awareness of CDD requirements was observed among DNFBPs compared to the financial sector. The applicable law has changed and the new analysis has been undertaken.

204. *Criterion 22.1* - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, CDD requirements detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs, except as explained below. Slovenia applies CDD requirements to all categories of DNFBPs under R.22. The APMLFT also covers additional types of DNFBPs, including traders in works of art, (Art. 4(1)20(o)) organisers and concessionaires organising games of chance (Art. 4(1)18), auctioneers (Art. 4(1)20(p)) and managers of bridging facilities set forth in the Act governing bridging insurance for professional and top athletes (Art. 4(1)12).

(a) Pursuant to point 1 of Art. 30(1) APMLFT, customers' identity shall be determined and/or verified each time they enter a casino or a gaming hall or access a safe. The APMLFT considers a player's online registration for participation in a game as an establishment of the business relationship, which triggers CDD (Art. 17 (4)). The APMLFT also requires full CDD measures to be applied by both land-based casinos and internet gambling providers upon payment of wins and bets over EUR 2,000 (point 3 of Art. 17(1)), to the extent that these measures have not been applied at the time of entry to the casino, online registration, or subsequently as part of ongoing monitoring.

The AMPLFT provides no specific measures to ensure that casinos are able to link the CDD information for a particular customer to transactions equal or above EUR 3,000. Only AML/CFT guidelines of the Gaming Supervision Office provide for the establishment of "mechanisms for linking customers to specific transactions in which the customer subsequently, in the process of games of chance, becomes engaged" (Sect. 4.1.1).

(b) Real estate agents are considered to be obliged persons under Art 4(1)20)(r) APMLFT. No specific provisions of APMLFT require real estate agents to apply CDD requirements with respect to both purchasers and vendors of property. AML/CFT guidelines issued by OMLP indicate that a real estate agent is expected to familiarize oneself with the relationship between the seller and the buyer of the property to identify potential dishonesty (Sect. 3.1).

(c) Traders in precious metals and precious stones or products thereof are considered to be obliged entities under Art. 4(1) 20 (n) and (o) APMLFT, but are also prohibited from accepting cash payments over EUR 5,000 (Art. 67 (1)) and payments in other currency than Euro (Euro Introduction Act Official Journal of the Republic of Slovenia, no. 114/06). Also, Art. 67 (1) stipulates that the limitation on accepting cash payments also applies when the payment is effected by several linked cash transactions exceeding a total amount of EUR 5,000. Thus, c.22.1(c) is not applicable for traders in precious metals and stones.

(d) The APMLFT applies to lawyers, law firms and notaries when they prepare for or carry out transactions for their clients concerning all activities listed in R.22 (d) (Art. 4 (2) and Art. 83 (1)) except for the buying and selling of business entities (other than companies).

Auditing firms and independent auditors, as well as legal entities and natural persons providing accounting or tax advisory services, are subject to the general CDD requirements (Art. 4 (1) 17 and 20 k). Auditing firms and independent auditors may apply simplified CDD measures when carrying out mandatory auditing of a legal entity's annual accounts except when reasons for ML/FT suspicion exist (Art. 57(6)).

(e) APMLFT subjects trust and company service providers (TCSPs) to the general CDD requirements when they prepare for or carry out transactions for their clients concerning all activities listed in R.22(e) by virtue of Art. 4 (20) (m) and Art. 3 (30).

205. *Criterion 22.2* - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, record-keeping requirements detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs. See R.11.

206. *Criterion 22.3* - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, PEP requirements detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs (See R.12). AML/CFT guidelines issued by supervisory bodies for accountants (Sect. 3.2.2 and 4.3.3) and notaries (Sect. 5.4.3 and 5.5) contain general references to PEPs as high risk customers and repeat corresponding APMLFT provisions. On the other hand, AML/CFT guidelines developed for casinos (Sect. 10.2.2) and real estate agents (Sect. 4.2.2) recommend more detailed procedures of identifying PEPs, including through internet-based searches and questionnaires. As regards lawyers, there are no specific AML/CFT guidelines issued related to PEPs.

207. *Criterion 22.4* - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, new technology requirements detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs (See R.15).

208. There is however no guidance issued for DNFBPs in relation to risks arising from the use of new products, business practices and technologies. The Decree on Detailed Conditions to be Met by Permanent Organizers of Classic Games of Chance stipulates that "technological processes must be designed in accordance with the gaming rules and must lay down the procedures for the identification of customers and transactions in respect of which there are grounds to suspect money laundering or terrorist financing, and the conduct of the operator" (Art. 10).

209. Criterion 22.5 - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, reliance of third party provisions detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs. See R.17.

Weighting and Conclusion

210. Slovenia is **LC** with R.22. Weaknesses identified in relation to FIs under R.10, 11, 12, 15 and 17 are also relevant for DNFBPs. There are also some additional deficiencies observed in respect of the underlying CDD requirements in R.10 related to casinos, real estate agents and legal professionals (Criterion 22.1).

Recommendation 23 – DNFBPs: Other measures

211. In the 4th round report Slovenia was rated largely compliant with R.16.

212. *Criterion 23.1* - Art. 4 of the APMLFT, which designates 'persons under obligation', includes all kinds of DNFBPs, including lawyers, law firms and notaries who are subject to a separate section in the Act (Chapter IV) explaining the application of obligations. Reporting requirements applied to DNFBPs are the same as for FIs, except as outlined below.

213. Art. 69(5) APMLFT imposes special reporting obligations – to report to the OMLP all cases where a customer seeks advice for ML or FT purposes - to auditing firms, independent auditors, legal entities and natural persons performing accounting or tax advisory services. A similar reporting requirement is applied to lawyers, law firms and notaries under Art. 83(2). Reports shall be submitted immediately and not later than three working days after seeking such advice.

214. Art. 84 APMLFT also provides for exceptions from reporting in relation to lawyers, law firms and notaries with regard to data obtained from, or about, a client in the course of establishing a client's legal position or when acting as a client's legal representative in judicial proceedings. This also includes advice on instituting or avoiding such proceedings, irrespective of whether such data is obtained before, during or after the proceedings. These exemptions are in line with client privileged information.

215. There are no specific exemptions from reporting requirements regarding precious metals dealers or trust and company service providers as allowed by the standard.

216. *Criterion 23.2* - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, internal control requirements detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs. See R.18.

217. *Criterion 23.3* - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, internal provisions dealing with higher risk countries detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs. See R.19.

218. *Criterion 23.4* - By virtue of Art. 4(1) and (2) and Chapter IV of the APMLFT, tipping off and confidentiality provisions detailed in the APMLFT apply to DNFBPs in the same way that they apply to FIs, except as provided for under Art. 122(6). This says that a lawyer, law firm, notary, audit company, independent auditor, person performing accountancy services or tax advisory services that seeks to dissuade a client from engaging in illegal activity will not commit a tipping off offence. See R.21.

Weighting and conclusion

219. Criterion 23.1 is met with other criterions mostly met. The most important criterion is 23.1 which is met and other deficiencies are of relatively minor importance. Deficiencies identified under Recommendations 18, 19 and 21 are also applicable to compliance with Recommendation 23. For these reasons **Slovenia is rated LC with R. 23.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

220. Previously Slovenia has been rated compliant with regard to then R. 33. It was mentioned however that there is a need to acquire updated information on the beneficial ownership and controlling shareholders particularly in respect of the larger companies and joint stock companies. Moreover, the necessity to continuously assess the risks inherent in the issuing and circulation of bearer shares and, as appropriate, manage those risks and/or implement changes in the policies adopted was mentioned. Since then, the FATF standard has changed substantially.

221. *Criterion 24.1* - Descriptions of different types, forms and basic features of legal persons, and processes for their establishment, are included in different laws guiding the types of legal persons (Companies Act, Associations Act, Foundations Act, Institutes Act, Cooperatives Act, Freedom of Religion Act, Political Parties Act, Representativeness of Trade Unions Act, etc.). The processes for recording of basic ownership information for different types of legal persons are set out most importantly in the Business Register Act (BRA) and Court Register Act (CRA). Entities obtain legal personality upon entry in the registers, except for foundations who obtain legal personality upon approval of their Deed of Establishment by the competent ministry (see under c.24.3). The APMLFT further describes processes for 'business entities' to determine their beneficial ownership information, maintain precise and up-to-date records on beneficial owners, and enter this into a central beneficial ownership register. The applicable rules vary between corporate entities (Art. 35) and entities with no business shares (Art. 36). However, entities have until November 2018 to comply with these obligations and the register has not been set up yet. Currently, the only process in full force to obtain and record beneficial ownership information of legal persons operating in Slovenia is through CDD procedures by obliged entities, which are described in the APMLFT (see under c.24.6).

222. Since the abovementioned information is contained in law, it is publicly available. Furthermore, information on registration of various types of legal persons and on obtaining of information on their basic ownership is publically available on governmental websites. APLRRS, the Agency that manages the Business Register, has such information on its website for both corporate and non-profit legal entities.[76] The website of the Ministry of Interior provides such information for associations and foundations in particular.[77]

[76] www.ajpes.si/.
[77] www.mnz.gov.si/si/mnz_za_vas/drustva_ustanove_shodi_prireditve/.

223. *Criterion 24.2* - In its NRAs, Slovenia has analysed the ML/FT vulnerabilities inherent in various financial and non-financial sectors, such as banking and insurance companies and casinos, and NPOs (which have legal personality mostly as associations, institutes or foundations) – although consideration of NPOs appeared very limited. The NRA also considered 1) the availability of independent sources of information on legal persons for LEAs and 2) corporate and trust transparency, as part of the assessment of national vulnerability to ML/FT. However, the ML/FT risks associated with all types of legal persons have not been comprehensively assessed.

224. *Criterion 24.3* - The Slovenian Business Register is a central database containing information about all 'business entities' involved in a profit or non-profit activity having their principal place of business located on the territory of Slovenia, as well as information on their subsidiaries and other divisions performing business activities in the country. It is managed by APLRRS. For businesses of sole proprietors and natural persons (e.g. landlords), the Business Register serves as the primary register (their business is directly registered in there). For all other business entities, it serves as a secondary register since these entities are first registered in their respective primary register or official records with another registration authority, and then the information is transferred into the Business Register.

225. Primary registration of many types of legal persons happens through the Slovenian Court Register of Legal Entities (hereafter: Court Register). As prescribed by the CRA, unlimited companies (d.n.o), limited partnerships (k.d.), limited liability companies (d.o.o.), public limited companies (also called joint-stock companies, d.d.), limited partnerships with share capital (k.d.d.), economic interest groupings (GIZ), limited liability co-operatives (z.o.o.), no-liability cooperatives (z.b.o.) and institutes are entered primarily in the Court Register. District courts carry out the data entry. Whenever the word 'company' is used hereafter, it includes 'partnerships', in line with Art. 3(3) CA. The requirements on cooperatives and economic interest groupings are not analysed separately under the criteria below. Cooperatives are traditionally established in the fields of agriculture and forestry, and risks for ML are seen as very low. Authorities further advised that their activities must be registered under the same rules as companies. Economic interest groupings are formed by one or more existing companies and are thus a 'secondary' form of legal person.

226. Registration of associations happens with local administrative units under the Ministry of Interior. Foundations must obtain approval of their Deed of Establishment by the Ministry competent for their field of activities. Upon receipt of the approval, the Ministry of Interior enters the foundation *ex-officio* in the register of foundations.

227. The relevant laws prescribe which information companies, institutes, associations and foundations must submit to registering authorities (Art. 4-5 CRA, Art. 47 Companies Act (CA), Art. 18 and 46 AA, Art. 14 FA, Art. 56-59 IA). This includes all basic information required under criterion 24.3.

228. All the above-mentioned information that is registered for companies, associations, foundations and institutes is publicly available online from the Business Register or upon request with the registering bodies pursuant to the Access to Public Information Act.

229. *Criterion 24.4* - **Companies** are not explicitly obliged to maintain themselves registers on shareholders/members/partners, but this information must be submitted to the Court Registrar and updated upon any change. A limited liability company is formed by a contract, the memorandum of association, which is signed by all members and which includes information on each member and their capital contributions and holdings (Art. 474, 478, 482 CA). The memorandum must also set out the associated voting rights; if not, the general provisions on voting of Art. 506 CA shall apply. An unlimited company is established by means of a contract of partnership between company members which governs the legal relations between them. An application for registration shall be done by all members and shall include the name of each company member. Unless agreed otherwise, members shall make equal capital contributions (Art. 76-78 CA; Chapter 27 of the Code of obligations on memorandum of association). A limited partnership is formed by a partnership agreement (Art. 135, 136, 137 CPC). Limited partners are not entitled to conduct the partnership's business. A notification

for entry in the register shall include the details of the limited partners and the amount of their contributions. The documents containing the information on shareholders and partners are submitted to the Court registrar and available through the Business Register.

230. The books of shares for public limited companies are held within the central registry of holders of dematerialized securities maintained by the Central Securities Clearing Corporation (CSCC) together with the holder's name and address (Art. 182, 235 CA, Art. 14(3), 25(1) Book Entry Securities Act (BESA)). The number of shares held by each shareholder of public limited companies is registered and every share has a designation if it bears voting rights or not. The nature of the voting rights is described in the articles of association of the company that are available through the Business Register.

231. **Associations** must have founding acts which stipulate regulating powers. There is no explicit obligation in the law to maintain information on membership. Authorities and the NPO umbrella organization advised that it is self-evident that an association must keep a list of members, otherwise it cannot be functioning in accordance with its statute and with the law, given that management decisions must be made by its members united in the general assembly at least once a year (Art. 1(2) and 13 AA). **Foundations** must adopt their rules and regulations, containing regulating powers, within 30 days of the issuing of the approval of the Deed of Establishment. Members of the first board of Trustees must be communicated to the register. **Institutes** must have a founding act containing basic regulating powers and must submit a list of the first members of the bodies of the institute to the court registrar (Art. 3 and 4 CRA).

232. *Criterion 24.5* - The registering courts (for companies and institutes) and administrative units within ministries (for associations and foundations) verify whether information submitted is complete and whether conditions for establishment and registration have been fulfilled (Art. 29-30, 34 CRA; Art. 19 AA, Art. 11 FA). In case of incomplete information or unfulfilled conditions, applicants are notified and can complete or alter the application within a certain deadline or it is otherwise rejected. Furthermore, certain documents to be submitted to the registering courts must be certified. For public limited companies, the Charter must always be prepared by a public notary. For limited liability companies, unlimited companies and limited partnerships, contracts of members or founders must be certified by a notary or by officials at 'one-stop-shops' for creation of companies. For institutes, the certification of signatures of founders in establishment acts must always be done by a notary. Notaries are obliged entities under the APMLFT when they assist clients in transactions concerning establishment and management of companies and management of shares (Art. 83 APMLFT), and must verify the identity of clients as part of CDD measures.

233. Companies and institutes must notify the court of changes to data that is registered within 15 days and enclose the acts that reflect the latest changes (Art. 47 and 48(3) CA; Art. 3(3) CRA; Art. 19 BRA). Transfers of shares for limited liability companies can only be made through a notarial deed (Art. 481(3) CA). For public limited companies, transfers of shares must be recorded in the share register (Art. 236 (3) CA) maintained by the CSCC and exercise of rights of shareholders is conditional on the information contained in the CSCC register. Changes in the entries of persons in the share books are performed by the CSCC on a daily basis following the transfer of shares between the securities accounts of different holders (Art. 25(2) BESA). If an association changes any of the registered basic information, it must lodge an application for a revision of registration within 30 days of making the alteration upon which the competent authority shall be obliged to decide within 30 days (Art. 20(1) AA). Depending on the type of change, changes in the data registered by foundations must be approved by the registering ministries or reported directly to the Ministry of Interior within 30 days of making the change (Art. 17-18 FA). There are no obligations on foundations to keep information on members of the Board of Trustees up-to-date.

234. *Criterion 24.6* - In cases where the legal owner (or founder/representative in the case of NPOs) is also the beneficial owner, the information in the Business Register would be relevant. The documents on shareholders and partners available through the Business Register and the shareholders register for public limited companies held by the CSCC can also contain relevant

information. In the specific case of listed companies and companies falling under the Takeovers Act, there are disclosure requirements for direct and indirect shareholdings (including through nominee accounts, see c.24.12) at several levels of ownership percentages, to the company and to the supervisor (Art. 105, 117-127, 134 FIMA).

235. For all other cases, Slovenia relies upon beneficial ownership information collected by FIs and DNFBPs in the course of CDD. This mechanism is only available insofar as a legal person has a business relationship with a Slovenian obliged entity. Although there is no legal requirement for Slovenian legal person to maintain such a relationship, the overwhelming majority of the most common type of companies does have a Slovene bank account. For the process of identification of beneficial ownership within CDD, see further under R.10.

236. As noted under c.24.1, the new APMLFT introduces the obligation for business entities (corporate and non-corporate ones) to collect and hold information on their beneficial owners and to set up and manage precise and up-to-date records on beneficial owners. It also foresees the establishment of a central beneficial owner registry (Art. 41, 44-45, 137(16) APMLFT). Yet these new are still in the phase of being set up and cannot thus not influence the rating (or the ratings of subsequent criteria). Business entities shall discover the data within one year following the entry into force of the new law and must enter the data into the registry within 14 months (thus by November 2017 and January 2018 respectively) (Art. 176 (1) and (2) APMLFT).

237. For the purposes of both CDD measures and the new beneficial ownership discovery requirements, the APMLFT defines beneficial owner as a natural person who ultimately owns or controls or otherwise exercises oversight of a customer, or a natural person on whose behalf a transaction is carried out or services performed (Art. 33 APMLFT). This broad definition is in line with the standard. Art. 35 and 36 APMLFT further define beneficial owners of corporate entities and entities with no business shares (such as associations, institutes and foundations). Although it is noted positively that the authorities provide further instructions in these articles on determination of beneficial ownership, some potential beneficial owners could be missed in application of these definitions. This relates in particular to natural persons who may exercise control through positions held within non-corporate legal persons, or natural persons who may control legal persons through other means, without providing funds.

238. *Criterion 24.7* - Obliged entities are required to monitor business activities undertaken by customers, which includes the verification and updating of customer information (Art. 49 APMLFT). The scope and frequency of the update depend on the assessed ML/FT risk to which the customer is exposed. In any case it should be conducted at least after the expiry of five years from the date of the last CDD if the customer has carried out at least one transaction through the obliged entity in the last twelve months. Although this is in line with the risk-based approach, it may thus not be ensured in all cases that up-to-date beneficial ownership information for all legal persons is available to competent authorities. Furthermore, this may lead to beneficial ownership information of customers who use products or services of obliged entities where transactions are infrequent, not to be updated.

239. The new APMPFT requires business entities to update their own records on beneficial owners in case of any changes (Art. 41 (3)). The business entities are also responsible for the accuracy of the data entered in the beneficial ownership register (Art. 44(5)). They are obliged to enter changes in the register within eight days (Art. 44(3)). The OMLP has been entrusted with the power to enforce the new obligations and to verify that business entities will enter accurate and up-to-date information.

240. *Criterion 24.8* - Companies, institutes, associations and foundations are required to have an authorised legal representative (a natural person). The authorities have advised that the Inspection Act stipulates the obligation of responsible persons to cooperate with competent authorities (Art. 19, 20, 23, 29). However, the representative does not need to be resident in Slovenia, thus enforcement of obligations to cooperate could be challenging.

241. *Criterion 24.9* - According to the general record-keeping provisions for obliged entities, data related to CDD shall be retained for 10 years after the termination of a business relationship or the completion of a transaction (Art. 129 APMLFT). Information on subject entries in the relevant registers is kept by the authorities competent for registration indefinitely (Art. 2(3) CRA; Art. 2 Protection of Documents and Archives and Archival Institutions Act; Decree on documentary and archival material custody).

242. The new APMLFT requires business entities to keep records of data on beneficial owners five years after the person ceases to be a beneficial owner. In case a business entity ceases to exist and does not have a known successor, the court or any other institution involved in its dissolution must order the records on beneficial ownership to be kept for five more years after the dissolution (Art. 41(4) and (5)). The authorities have advised that, since it would be difficult to suggest one solution for all various types of legal entities, the APMLFT leaves the decision on where the records will be kept to the court or any other institution involved in its dissolution.

243. *Criterion 24.10* - The general powers of the OMLP to request CDD information from obliged entities in case of grounds for ML/FT suspicions may be relevant in this regard, as far as a legal person has a business relation with a Slovenian obliged entity (Art. 91-93 APMLFT). Furthermore, in the case of suspicions, the OMLP has the power under Art. 94 APMLFT to require from any natural or legal person under Slovenia's jurisdiction to submit data, information and documentation needed for detecting and proving ML, FT or related predicate offences, which could include information to determine beneficial ownership. The deadline to provide information in both cases is 15 days but the OMLP can set a shorter time limit if necessary.

244. Powers of LEAs under the CPC to obtain records in the course of investigations are also relevant (see R.31). FI and DNFBP supervisors have powers to request information needed to perform supervision (see R. 27). LEAs and other public authorities with a legitimate interest can also get access to information held in the Business Register and CSCC Register that is not publically available. This includes ID-numbers and other personal data of shareholders, authorized representatives and members of the boards.

245. The new APMLFT has introduced the obligation for legal entities to 'immediately' provide data on their beneficial owners when required by LEAs, courts and supervisory bodies (Art. 42). This provision cannot be used yet since entities have until November 2017 to comply with the obligation to discover their beneficial owners. LEAs, courts and supervisors will be provided with free access to the envisaged beneficial ownership Register and electronic search tools for the purpose of ML/FT prevention and detection (Art. 44, 46(4) APMLFT).

246. *Criterion 24.11* - In the 3rd round, it was indicated that bearer shares are not prohibited in Slovenia. With regard to public limited companies, Art. 175 CA still stipulates that shares can be made out to the bearer or to the name. However, Art. 182 CA adds that all shares must be issued in book-entry form in line with the provisions of the Act regulating book-entry securities. The CSCC have advised that 'book-entry form' means that shares must be issued in dematerialized form and shareholders must be registered with the CSCC. There is no obligation on holders of bearer shares issued in the past to register, but the authorities have advised that no rights can be exercised on these legacy bearer shares until they are registered. Authorities further advised that bearer share warrants cannot be issued under the Slovene legal framework.

247. The APMLTF contains additional mitigating measures regarding bearer shares. Obliged persons are prohibited from establishing a business relationship or carrying out a transaction with a customer that is a legal person that has bearer shares which are not traceable through a register or business documentation (Art. 65).

248. *Criterion 24.12* - Nominee shareholding by lawyers, notaries, legacy custodians, special custodians, insolvency managers and other persons providing custodian services in the scope of their regular activity or occupation is enabled for public limited companies. Brokerage companies can keep securities on a fiduciary account opened for a client who is such a person. The client

(nominee) must be the legal holder of the securities credited to such an account on behalf of one or more other persons (the nominators) (Art. 255 (4) and (5) FIMA). By the account type, it is revealed that the holder acts as a nominee. Information on the type of the account is available to the brokerage company who operates the account, to the CSCC and to the issuer of the securities.[78] Art. 256 FIMA stipulates that prior to opening a client's account, a brokerage company shall be obliged to verify that client's identity in a reliable manner. Brokerage companies are obliged entities under the APMLFT and thereby also required to identify and verify the identity and beneficial ownership of their customers. Lawyers and notaries (as far as they assist in planning or executing transactions for clients concerning managing of securities and opening or managing of securities accounts) are also obliged entities and must conduct CDD. However, the group of persons that can act in the capacity of nominee shareholder is not restricted. Moreover, it appears that the nominee has the discretion to request the brokerage company to open a special fiduciary account, and that it could also request to open a normal client account. Thus, the possibility for brokerage companies to open a fiduciary account for nominee shareholders does not amount to a full disclosure requirement comparable to the mechanisms under criterion 24.12. Furthermore, there appear to be no disclosure requirements on the nominee if a nominee would hold securities for a nominator without the intermediation of a brokerage company. However, the authorities advised as an additional mitigating measure that for public limited companies whose securities are admitted to trading on a regulated market (and other companies that fall within the scope of the Takeovers Act), the duty for shareholders to report shareholding over certain thresholds to the company and to the SMA includes shares held indirectly through a nominee account (Art. 105, 117-120, 134 FIMA).

249. Authorities advised that nominee holding of shares in other types of companies (i.e. shares that are not issued in the form of securities, but are registered in the Business Register) is not legally recognized. Therefore, they advised that in case of "fiduciary" holding of such shares Art. 50(1) Code of Obligations would apply which provides that fictitious contracts are void *inter partes*.

250. The issue of nominee directors is not addressed under Slovenian law. In the absence of a prohibition on nominee directorship, it is concerning that there are no mechanisms to prevent their misuse, given that 'straw men' are a relevant risk factor for Slovenia.

251. *Criterion 24.13*– Fines can be imposed on a company that does not submit data to be included in the application for registration, does not report data and documents that reflect the actual situation, or does not notify the court registrar of any changes in registration data (Art. 685 (1) CA). The level of fines is proportionate to the size of the company: EUR 15,000 to 45,000 for big companies, EUR 10,000-30,000 for medium-sized companies, EUR 2,500 to 15,000 for small companies and EUR 1,000-6000 for micro companies. Responsible persons can be fined between EUR 500 and 4,000 for these offences (Art. 685 (2) CA). The same range of fines can be imposed on public limited companies for not issuing shares in book-entry form (Art. 685 (1) point 7 CA). No other sanctions than fines can be imposed on companies for breaches of the registration requirements under the Companies Act. In case of submitting false documents to support registration applications, Art. 251 of the Criminal Code provides for two years of imprisonment for forgery of documents with criminal intent.

252. Associations, foundations and institutes can be fined EUR 420, EUR 600, and EUR 2,000 to EUR 4,000 respectively for failure to report changes in registration data to competent authorities within 30 days (Art. 53(2) AA; Art. 35(2) FA; Art. 19, 25 BRA). Foundations can also be fined for failure to submit their regulations to the competent authority within three months (Art. 35(3) FA). Responsible persons of associations, foundations and institutes can be fined EUR 125, 200, and 200-400 EUR respectively for these misdemeanours. There are no sanctions for failure to submit data to be included in application for registration but incomplete applications would be rejected (see c.24.5).

[78] A recent amendment to the Dematerialized Securities Act that entered into force after the on-site visit has extended the availability of this information to the public.

253. There are no sanctions prescribed under the APMLFT that can be imposed on legal persons and their representatives for failure to provide information requested by the OMLP under Art. 94 APMLFT. Authorities advised that in general, minor offense proceedings can be started under the Inspections Act on legal persons and their representatives for failure to cooperate with competent authorities, with available fines of EUR 1,500 for the legal person and EUR 500 for the representative.

254. The SMA can impose a proportionate range of supervisory measures and sanctions on listed companies and legal and natural persons as direct or indirect shareholders for failure to comply with reporting and publication duties of shareholding over the thresholds (Art. 146, 558, 559 FIMA). There appear to be no sanctions available under FIMA for brokerage companies for failure to verify the identity of their client; however such sanctions are available under the APMLFT in the context of CDD (see under R.35).

255. With regard to the CDD requirements which form the current mechanism to obtain beneficial ownership information, sanctions are available under the APMLFT (see R.35).

256. Art. 167 APMLFT prescribes fines of EUR 6,000 to EUR 60,000 on legal entities that fail to comply with the new beneficial ownership obligations once they become enforceable (for failure to discover the data or discovery of false data; failure to maintain precise records; failures to keep information for 5 years following termination of beneficial ownership status; failure to furnish information to authorities without undue delay; failure to enter (changes in) data or entering of false data in the register within eight days). The sanction for failure to enter (changes in) data within eight days may not be fully proportionate, as it could be very challenging for business entities to comply with this deadline in case of complex ownership structures.

257. *Criterion 24.14* - Parts of the basic information in the Business Register can be viewed in English. The online public part of the CSCC Register, which is also available in English, contains some information on shares issued by a company (number of shares, number of shareholders, and percentage of foreign shareholders). To obtain other information, foreign authorities can use mechanisms of international cooperation. The OMLP assists foreign counterparts by sharing the information available to the OMLP, including on beneficial ownership, based on general provisions on international co-operation (Art. 104-113 APMLFT). Public prosecutor's offices and courts can handle incoming requests for assistance, which may relate to beneficial ownership information. See also the analyses for R.37 and R.40.

258. *Criterion 24.15* - According to the authorities, the quality of assistance received from other countries in response to requests for beneficial ownership information is not monitored.

Weighting and Conclusion

259. Slovenia meets or mostly meets most of the criteria under R.24. The availability of basic information is at a high level. Competent authorities currently rely on obliged entities to obtain information on the beneficial ownership of legal persons. There are some minor gaps in this mechanism, in case a legal person does not have a business relation with a Slovene obliged entity, or when beneficial ownership information collected by obliged entities is not updated frequently enough in case of low-risk customers. Furthermore, there are some gaps in the mechanisms to ensure that nominee shareholders are not misused. Slovenia has not assessed ML/FT risks inherent to all types of legal entities that may be established in the country. The new APMLFT introduced an obligation on legal persons themselves to discover and record beneficial ownership. This obligation and related measures were analysed under relevant criteria above, but due to the transition period for compliance until November 2018, they did not influence the rating. **Slovenia is rated LC with R.24**.

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

260. Former R.34 was considered as not applicable to Slovenia in the 3rd round MER, since trusts cannot be established under Slovenian law. However, the new R.25 contains requirements on all countries, irrespective of whether the country recognises trust law.

261. Trusts still cannot be formed under Slovenian law. Slovenia is not a Party to the Hague Convention on Laws Applicable to Trusts and their Recognition. Yet it appears that there are no provisions precluding trusts or similar legal arrangements established under foreign law from conducting their activities through the Slovenian financial system, and no prohibitions for persons under the jurisdiction of Slovenia to act as trustees or provide other trust-related services. Legal and natural persons providing trust and company services in Slovenia are obliged entities under the APMLFT (Art. 4(1) point 20m). The APMLFT defines TCSPs as any natural person or legal entity which by way of business provides to third parties any of the services listed in the law, which includes 'acting as, or arranging for another person to act as, a trustee of a foundation, trust or similar foreign law entity which receives, manages or distributes property funds for a particular purpose' (Art. 3 point 30). Authorities have advised that no business has been established to provide trustee services. The evaluation team did not find any information on-site or from public sources suggesting otherwise. The authorities maintain that TSCPs were only included in the scope of the APMLFT in case the situation would change in the future.

262. The evaluation team identified a Slovene type of legal arrangement that would fall under R.25. It concerns mutual investment funds which are not a legal entity. They are a form of UCITS funds, set up in line with the EU Directive 2009/65/EC on undertakings for collective investment in transferable securities (UCITS), and regulated under the Slovene Investment Funds and Companies Act (IFCA, last amended in 2011). A mutual fund represents assets which are separate from the assets of the management company managing this fund and are owned by the holders of investment coupons of the mutual fund. Mutual funds can be set up only by a management company, who must conclude a contract on the management of custodian services with the custodian (depositary). The authorities have stated that this means a licensed management company as indicated in the UCITS directive. They must obtain approval to manage an investment fund by the SMA (sections 3.2.1, 7.8 IFCA). Investment funds are obliged entities under the APMLFT as 'investment funds that sell their own units' in Slovenia. If the investment fund does not manage itself, which is the case for mutual funds, then the manager of the fund is are responsible for compliance with the requirements of the APMLFT on obliged entities (Art. 4 (1) point 6 APMLFT).

263. *Criterion 25.1* - This criterion is not applicable to Slovenia as far as trusts are concerned, since there is no trust law.

264. As obliged entities under the APMLFT, managers of mutual funds are obliged to determine and verify the identity of their customers and their beneficial owners (see R.10). The fund must have a contract for custodian services with a regulated entity as its depositary, e.g. a bank holding a license for depositary services by the BoS. If a management company delegates the performance of individual services or operations involving the management of individual investment funds to another person, it must do so in writing (Art. 122 IFCA). Record-keeping requirements under the APMLFT comply with sub criterion c) on maintaining of information on the investors for at least 5 years (see R.11). Moreover, management companies shall keep and store records and documents concerning all services provided and transactions carried out in a manner enabling supervision of its operations (Art. 69 IFCA). For each mutual fund under management the management company shall keep records of holders of investment coupons, with their company name or personal name and address (Art. 226, 231 IFCA; Decree on Operations of the Management Company).

265. *Criterion 25.2* - This criterion applies to trusts insofar as foreign trustees establish a business relationship with a Slovenian FI or DNFBP. Obliged entities are required to conduct CDD on their customers, including verification of their identity and determination of their beneficial owner (see R.10 and R.22). Art. 37(1) APMLFT specifies that the beneficial owner of a foreign trust or similar foreign law entity means natural persons who are the founders, trustees, beneficiaries, protectors,

and any other natural persons who in any other way directly or indirectly control the property of such an entity. Basic CDD record-keeping requirements are applicable (Art. 129) which are in line with c.25.1(c). Data on the beneficial owner that shall be kept by obliged entities consists of personal name, permanent or temporary address, date of birth, nationality and the amount of ownership interest or any other type of control (Art. 137 (1) point 14). If the beneficial owner of a foreign trust or similar entity includes a category of persons with yet to be determined exact beneficiaries, the obliged entity shall acquire sufficient data and information to establish and verify their identity at the time of payment (Art. 19(3) point 2).

266. FIs and DNFBPs must update customer information, including data on beneficial ownership (Art. 49 APMLFT). The scope and frequency of the update depend on the customer's exposure to ML/FT risks. In any case, it should be conducted at least after the expiry of five years from the date of the last CDD if the customer has effected at least one transaction with the obliged entity in the last twelve months. Although this is in line with the risk-based approach, it may thus not be ensured in all cases that up-to-date beneficial ownership information for all legal persons is available to competent authorities. Furthermore, this may lead to beneficial ownership information of customers who use products or services of obliged entities where transactions are infrequent, not to be updated.

267. In the case of investors in mutual fund arrangements, the managers of mutual funds are also required under IFCA to keep all relevant information on investors.

268. *Criterion 25.3* - There is no requirement for trustees themselves (professional or otherwise) or for managers of mutual funds acting on behalf of underlying investors to disclose their status when forming business relationships with obliged entities or carrying out a one-off transaction. Nor is there an all-encompassing obligation on obliged entities to obtain a statement from their customers whether they are acting on behalf of third persons. Such a statement is only required in case of an (occasional) transaction above determined thresholds (Art. 24(2) & 25(2) in combination with Art. 17 (1) point 2 & 3 and Art. 18 APMLFT). Requirements to determine beneficial owners of customers could to some extent mitigate this deficiency.

269. *Criterion 25.4* - There are no legal provisions which would prohibit or prevent the disclosure of information by trustees of foreign trusts or managers of mutual funds.

270. *Criterion 25.5* - The members of the mutual fund management company's board and the company's employees shall provide the SMA at its request with reports and information on all matters of importance for supervision (Art. 460 IFCA). Depositaries of management funds must provide to the SMA, at its request, reports and information on all matters relevant for supervision of the performance of the depositary function for investment funds (Art. 158(1) IFCA).

271. The OMLP can obtain information from managers of mutual funds, who are obliged entities under the APMLFT. These powers are also relevant in relation to trusts, as far as a party to a foreign trust enters into a business relationship with a Slovenian obliged entity. When there are grounds to suspect ML or FT, the OMLP has powers to request CDD information from obliged entities and data on the assets and other property of a person in respect of which there are grounds to suspect ML or FT (Art. 91-93 APMLFT). This includes beneficial ownership information and information on address and registered office of the customers (Art. 137 APMLFT). In case of suspicions, the OMLP can also require data, information and documentation from any person if needed for detecting and proving ML, related predicate offences and FT (Art. 94 APMLFT).

272. The police can, upon court order or in some specific instances upon their own initiative, order a bank, savings bank, payment institution or an electronic money company to disclose information and documentation on a suspect or related persons (Art. 156 CPC). Although there are no similar powers for the police to require other FIs or DNFPBs to produce customer records, authorities can use other relevant powers under the CPC to conduct searches of premises and seize documents to reach the same result (see R.31). The laws regulating supervision by BoS, ISA and SMA grant them powers to compel production of information by FIs (see R.27).

273. In addition, the new APMLFT introduces an obligation for 'business entities', including foreign law entities which accept, administer or distribute funds for particular purposes, to maintain up-to-date information on their beneficial ownership and to submit this information without delay to LEAs, courts or supervisory bodies. This information shall also be entered in a register of beneficial ownership, to which competent authorities will have access free of charge (Art. 41(2), 42, 44(3)). These obligations exist only 'if tax liability arises from their business activity'. Tax liability would arise if trust parties perform business activity relevant for the trust in Slovenia. Business entities have up until one year following the entry into force of the new APMLFT to discover this data (November 2017) and up until 14 months to enter such data in the Register (January 2018). It must be noted that sole proprietors and natural persons performing an activity independently are exempted from this obligation, so not all persons acting as a (professional or non-professional) trustee would fall under the scope. Furthermore, it remained unclear to the assessment team on whom exactly the obligation to maintain, record and register beneficial ownership information for trusts would lie.

274. *Criterion 25.6* - General provisions on international cooperation (under the CPC and under Art. 104 – 113 APMLFT) could be used to exchange information on trusts, mutual funds and similar legal arrangements administered in the country. The OMLP can submit data, information and documentation on customers or transactions in respect of which there are grounds for suspicion of ML or FT, which were acquired or retained in accordance with the provisions of the APMLFT, to a foreign FIU, upon the latter's request and under reciprocity. Furthermore, the OMLP and other supervisory bodies can cooperate with competent supervisory authorities of EU Member States and third states (Art. 139, 156-157 APMLFT). See also the analysis under R.40.

275. *Criterion 25.7* - Companies managing mutual funds are liable for failure to comply with AML/CFT requirements and can be fined under the APMLFT (see R.35). In case professional TSPs would start operating in the country, they would also be liable under the APMLFT. Art. 167 further establishes sanctions (6,000-60,000 EUR fine) for business entities, including foreign trust entities with tax liability in Slovenia, for failure to obtain, keep and update information on their beneficial ownership, once that obligation becomes legally enforceable. However, as outlined above, it is not clear on whom the obligation would exactly rest in the case of foreign trusts and thus who can be sanctioned. There are no other provisions with regard to legal liability or sanctions applicable to trustees since there are no legal obligations stipulated for them.

276. Mutual fund management companies can be fined between EUR 400 and EUR 250,000 (small companies) or between EUR 2,000 and 500,000 (medium and large companies) for failure to meet their obligations under IFCA; responsible persons can be fined between EUR 400 and EUR 10,000 (Art. 512, 514 IFCA). If a company repeatedly violates the rules, the authorisation for the company to manage investment funds can be withdrawn (Art. 478 IFCA).

277. *Criterion 25.8* - Sanctions on FIs and DNFBPs for failure to grant the OMLP timely access to requested information are stipulated in Art. 163(1) point 28 APMLFT (fine of EUR 12,000 - 120,000). FIs and DNFBPs can also be sanctioned for failure to provide information requested by supervisors in the exercise of their powers (see R.27, R.28, and R.35).

278. Depositaries shall be imposed a fine between EUR 400 and EUR 250,000 (small depositaries) or between EUR 2,000 and EUR 500,000 (medium and large companies) for failure to submit requested information to the SMA; on their responsible persons a fine between EUR 400 and EUR 10,000 can be imposed (Art. 516 IFCA).

Weighting and Conclusion

279. There are measures in place to ensure the availability of basic information on relevant parties in mutual funds (a Slovene type of legal arrangement, managed by asset management companies). With regard to foreign trusts, which can act through the Slovenian financial system, there are concerns with regard to the absence of a legal obligation on trustees to disclose their status, although requirements to determine beneficial ownership can mitigate this gap to some extent. With regard to

beneficial ownership information on mutual funds and foreign trusts, CDD obligations are relevant, although information obtained through this mechanism may not always be up-to-date in case of low-risk customers. **Slovenia is rated LC with R. 25.**

Recommendation 26 – Regulation and supervision of FIs

280. In the 4th round MER Slovenia was assessed to be largely compliant with former recommendation 23. The supervisory framework for the insurance sector was deemed to be inadequate.

281. *Criterion 26.1* - BoS, SMA and ISA are responsible for the supervision of FIs, including for AML/CFT requirements (Art. 151 APMLFT);

282. Art. 142 authorises the OMLP to supervise all obliged entities regardless of the existence of other regulators.

283. *Criterion 26.2* - Core principles institutions are required to be licensed. Other types of FIs are required to be licensed or authorised (Art. 4 and Art.95 of Banking Act; Art. 17 and 136 PSS; Art. 6 of the Foreign Exchange Act (FEA); Art. 135 of Alternative Investment Fund Managers Act (AIFMA); Art. 131, par. 1 of AIFMA; Article 113 of the Insurance Act (IA) and Article 118/2 of the IA)

284. *Criterion 26.3* - Art. 38 and 53 of BA requires members of the management and supervisory boards to, amongst other things, enjoy the reputation and possess the traits required to manage a bank's operations, and their conduct does not raise doubt about their ability to ensure the safe and prudent management of a bank's operations in accordance with risk management rules, professional diligence and the highest ethical standards, and the prevention of conflicts of interest and paragraph (2) of Article 38 of BA stipulates that a person is deemed not to enjoy the reputation and possess the traits required to manage a bank's operations if: 1. they have been convicted of a criminal offence and the conviction has not yet been expunged from the records; or they have been charged with a criminal offence prosecuted ex officio and for which a prison sentence of a year or more may be imposed.

285. Qualifying holders of bank shares must fulfil the conditions set out in Art. 66 and 68 of the Banking Act that includes, amongst others an assessment of "their reputation" and if there is a reason to suspect that an act of ML or FT, as set out in the APMLFT, was or will be committed or an attempt to commit such an act was or will be carried out in connection with the acquisition of a qualifying holding; or that the acquisition in question will increase the risk of money laundering or terrorist financing as set out in the APMLFT. If the qualifying holder is a legal person they must provide the BoS with the complete ownership structure and this information will be considered as part of the assessment of the application.

286. As regards the payment institutions and electronic money institutions and MVTS, Art. 26 PSSA, that sets out requirements from managers does not stipulate any measures that can prevent criminals and their associates from obtaining management positions. Section 27 requires BoS to assess holders of qualifying holdings (10% and above) for reasons of ensuring sound and prudent governance of a payment institution, in addition, the holders of qualifying holdings of a payment institution shall be only persons that are considered as appropriate by the estimation of BoS. BoS shall assess the appropriateness of holders of qualifying holdings in the light of performance and influence of a holder of qualifying holdings on the sound and prudent governance of a payment institution. And they shall consider the legal organisation form and activities that the holder provides, his/her financial positions and other characteristics.

287. As regards the exchange offices, Art. 9 FEA stipulates that a license shall be refused if BoS shall refuse to issue an authorisation if: the qualified owner of the currency exchange operator has been finally convicted of a wilful criminal offence prosecuted ex officio, or of one of a list of criminal offences committed out of negligence: concealment and the penalty has not yet been expunged from the criminal records; the responsible officer of the currency exchange operator has been finally convicted of one of the specified criminal offences and the penalty has not yet been expunged from

the criminal records;. the available information suggests that the activities and transactions that the qualified owner or responsible officer of the currency exchange operator would undertake or the actions that the aforementioned person has undertaken could impact the legality of the currency exchange operator's operations.

288. BoS is responsible for assessing the suitability of holder of qualifying holdings of electronic money institutions (Art. 27 (3) PSSA).

289. The Insurance Act contains similar provisions regarding insurance companies. Art. 19b refers to the requirements of a qualifying holder of an insurance company which are similar to the requirements by banks and Art. 24 lays out the requirements from a board member who must, amongst other things, meet the following requirements; characteristics and experience needed to manage the operations of an insurance undertaking, has not been convicted of a criminal offence committed wilfully or of one of the following criminal offences committed through negligence, negligent homicide, aggravated bodily harm, grievous bodily harm, endangering safety at work, concealment, disclosure and unauthorised acquisition of a trade secret, money laundering, disclosure of an official secret, causing public danger, and the conviction has not yet been deleted.

290. Financial service providers such as brokers and portfolio managers must fulfil the requirements set out in sections 155a and 157 FIMA regarding ownership and management functions and these sections refer to the relevant articles of the banking act that apply Mutatis mutandis.

291. *Criterion 26.4* - (a) A review of the Financial System Stability Assessment published by the IMF in 2012 indicates that Slovenia met the core requirements regarding core FIs at that time. (b) Other FIs are subject to supervision of the implementation of the provisions of the APMLFT (Art. 139) taking account of ML/FT risks (Art. 140).

292. *Criterion 26.5* - Art. 140 APMLFT imposes an obligation to competent supervisory authorities to consider a risk-based approach when they conduct supervision. According to Art. 140 (2) of APMLFT the following factors should be taken into account in the process of planning and conducting the frequency, scope, intensity of supervision data on AML/CFT risk as they were identified within NRA; data on specific national or international risks associated with clients, products or services; data on risk exposure of particular obliged entity and any other available data; all significant data associated with the particular obliged entity, including the information on any changes which are significant for obliged entity and its business activities. The elements set out in c. 28.5 are covered by the law. Currently BoS has implemented a risk based approach to supervision however they have not formally adopted a procedure for its implementation. Other supervisors do not apply a risk based approach and have not adopted the necessary procedures have procedures in place for supervision that takes account of all the factors specified in Art. 104 (2) under this new legislative requirement.

293. *Criterion 26.6* - There is a legal requirement for supervisors to take into account data concerning the risk of individual obliged persons, and other available data and important events or modifications related to the management of the obliged person, and any change of activities (Art. 140 (2)). However there is no explicit requirement for supervisors to review the assessment of the ML/FT risk profile of a FI or group (including the risk of non-compliance) periodically.

Weighting and Conclusion

294. c.26.1, c.26.2, c.26.4 and c.26.5 are met, c.26.3 and c.26.6 are partly met. Fit and proper requirements do not apply to beneficial owners in all situations and there is no explicit requirement for supervisors to review the assessment of the ML/FT risk profile of a FI or group (including the risk of non-compliance) periodically. **Slovenia is rated PC with R.26.**

Recommendation 27 – Powers of supervisors

295. In the 4th round evaluation Slovenia was rated partially compliant with the previous R.29. The applicable law has changed, so the new analysis has been undertaken.

296. *Criterion 27.1* - Art. 139 APMLFT grants the relevant supervisors the legal basis for supervising the respective bodies under their responsibility, for ML/FT purposes stating that supervision of the implementation of the provisions of this Act and the ensuing regulations shall be exercised within their competencies . The same article also provides the supervisors with the authority to order measures to remedy the irregularities and deficiencies within a time limit that it specifies; carry out proceedings in accordance with the law regulating offences; propose the adoption of appropriate measures to the competent authority; order other measures and perform acts for which it is authorised by law or any other regulation.

297. *Criterion 27.2* - Art. 139 APMLFT allows the relevant supervisors to use their existing powers to conduct supervision for AML/CTF purposes. BoS has extensive supervision powers from Section 8 of the BA which includes the authority to conduct on-site inspections in banks. Their power to conduct on-site inspections in other payment service providers and exchange offices is derived from Art. 184, and 187 to 191 PSSA and Art. 13 FEA, respectively. ISA derive their authority to conduct inspections from Section 7.1 of the IA (supervision of insurance undertakings), namely Art. 271 to 284. SMA derives its authority to conduct inspections from Art. 296 to 309 FIMA. In addition, the OMLP has authority to conduct inspections according to Art. 142 APMLFT.

298. *Criterion 27.3* - The above mentioned laws regarding the supervisory powers of the BoS, the ISA and SMA also grant them the power to compel production of information without a court order. As regards the banking sector, supervisory provisions are defined in the BA and from Art. 240 and 241 it is clearly evident that bank is obliged to submit all data and documentation which is needed for the purpose of supervision. In addition to that Art. 247 BA regulates the bank's obligation to ensure adequate access to data and documentation which are maintained in electronic form. With regard to the securities sector, Art. 296 to 309 FIMA give a power to SMA to compel production of information without a court order.

299. As regards the ISA, Art. 100 IA holds that upon their request another supervisory authority shall submit all information on an insurance undertaking or another supervised financial undertaking or another supervised entity required to perform the supervisory tasks of this undertaking or entity in the procedure for issuing authorisations or decision making on other matters.

300. Art. 146 holds that upon request, an insurance undertaking shall submit information needed to carry out supervision to the ISA. This information shall include amongst others the information necessary to take suitable decisions arising from the exercise of the rights and obligations of supervisors.

301. Furthermore, in accordance with Art. 101 IA, ISA shall collect and process information on facts and circumstances relevant to the performance of its tasks and powers stipulated by this Act.

302. In addition to that, Art. 141(3) APMLFT states that obliged persons shall submit to the OMLP in writing the data, information and documentation on the performance of their duties as provided under the Act, as well as other information which the OMLP requires for supervision, within eight days of receiving the request. Art. 146(1) also explains that an OMLP inspector shall be able to: (i) inspect internal acts, books of account, business correspondence, records and other data and documentation; and (ii) require clarification concerning facts or documents.

303. Criterion 27.4 - Art. 139 (3) APMLFT grants all supervisors the power to impose sanctions for failure to comply with AML/CFT requirements. Powers are considered under c.35.1.

Weighting and conclusion

304. All of the 4 criteria are met. **Slovenia is rated C with R.27**

Recommendation 28 – Regulation and supervision of DNFBPs

305. In the 4th round evaluation Slovenia was rated largely compliant with the previous R.24. It was stated in the report the risk based approach is at its initial stages. The applicable law has changed, so the new analysis has been undertaken.

306. *Criterion 28.1* - (a) In accordance with Art. 3(2, 3) Gaming Act (GA), games of chance can only be conducted by concession holders or on the basis of permission received from the competent authority, which is the Government of the Republic of Slovenia and under its authority the Minister of Finance.

(b) In accordance with Art. 85(a) and 93 GA, managers and key staff of casinos are required to be free of convictions related to crimes against life and body, human health, assets, economy, legal transactions, official duty and public authority or public peace and order. Online gambling can only be provided by someone who has a concession for a casino according to Art. 3(a). There are no provisions regarding lack of convictions with regard to shareholders in casinos however Art. 55(a) limits ownership to the government of Slovenia, companies 100% owned by the government, local communities, and public limited companies that are limited to a 20% holding each. The publically listed company cannot have more than 49% shares in the hands of natural persons and no one natural person can hold more that 10% of its shares. However there is a possibility that a natural person will control 20% of the shares of a casino through a wholly owned private company that controls the public company, without any screening.

(c) In accordance with Art. 151(4) APMLFT, FARS is responsible for supervising organisers and concessionaires organising games of chance, including where offered on the internet or other electronic means. In addition, Art. 141 APMLFT states that the OMLP shall perform supervision of the implementation of the provisions of the APMLFT.

307. *Criterion 28.2* - Art. 151 APMLFT appoints various supervisory bodies to be responsible for AML/CFT supervision of non-casino DNFBPs. These are: (i) MIRS for real estate agents and traders in precious metals and stones (those these are not considered to be DNFBPs under the FATF definition; (ii) the Bar Association of Slovenia for lawyers and law firms; (iii) the Chamber of Notaries of Slovenia for notaries; and (iv) APOA and the Slovenian Institute of Auditors for auditing firms and independent auditors. In addition, FARS is responsible for implementation of prohibitions against the acceptance of payments for goods and services in cash in an amount exceeded EUR 5 000. Sectorial supervisory bodies are not designated under Art. 151 for persons carrying on accounting services or tax advisory services, or for TCSPs. However, Art. 141 APMLFT states that the OMLP shall perform supervision of the implementation of the provisions of the APMLFT.

308. Criterion 28.3 - Art. 142 APMLFT designates the OMLP as a supervisor for all obliged entities in addition to designated supervisors if they exist, however the OMLP has not yet put in place the mechanism for monitoring compliance by other DNFBPs.

309. Criterion 28.4

(a) Art. 139 to 150 APMLFT give the OMLP powers to perform its functions, including powers to monitor compliance. Art. 139 and 151 APMLFT require sectorial supervisors to use their respective supervisory powers for exercising supervision over the implementation of the APMLFT. Art. 111 of the Notaries Act empowers the Chamber to conduct inspections.

(b) Auditors and people in management positions in audit firms must not have been convicted of a crime against property crime or an economic crime that has yet to be expunged from the record (Art. 48 Auditors Act) and Art. 61 of the Act stipulates that at least 75% of shares in an audit firm must be held by auditors. However, there are no provisions for the remaining 25%. The Bar Act (Art. 27 and 30) assert that in order to get a license a lawyer must show that he is reliable in practising the legal profession and has not been convicted of a criminal offence which makes him morally undeserving to practice law and a law firm (Art. 4). According to Article 113.c of the Notary Act, in case of a final conviction for a criminal act related to the performance of notarial work and in case of a final

conviction for any premeditated criminal act with the penalty of at least six months of prison, a disciplinary measure of a permanent prohibition to perform the notarial work can be applied. The authorities have not provided details of measures in place to prevent criminals or their associates from being accredited, holding or being the beneficial holder of a significant or controlling interest or holding a management function in real estate agents, or TCSPs.

(c) Sanctions available are explained under R.35.

310. *Criterion 28.5* - Art. 140 of APMLFT now requires a risk-based approach to supervision and lists the factors to be taken into account when planning the frequency, scope, intensity and implementation of supervision (though not all of the elements set out in c.28.5 are covered). However, the authorities have not implemented or prepared procedures for supervision under this new legislative requirement. The Bar Association randomly selects lawyers and law offices every year based on responses to a questionnaire, which receives few responses**.** Chamber of Notaries regularly supervises the work of notaries but it is not based on risk assessment and this is true of the market inspectorate and FARS as well. The OMLP has not yet started using its recently acquired supervisory powers.

Weighting and Conclusion

311. The basic infrastructure for sound regulation and supervision of DNFBPs has gaps (c.28.1, c.28.3) and there is also weakness in the implementation of a risk based supervisory approach (c.28.5). **Slovenia is rated PC with R.28.**

Recommendation 29 - Financial intelligence units

312. Slovenia was rated compliant with the former R.26. The applicable law has changed, so the new analysis has been undertaken.

313. *Criterion 29.1* - The OMLP is a constitutive part of the Ministry of Finance. In accordance with Art. 87 APMLFT, the OMLP performs duties related to the prevention and detection of money laundering, predicate criminal offences and terrorist financing. It acts as a national centre for the receipt and analysis of reports on suspicious transactions and other data, information and documents related to potential money laundering, predicate offences or terrorist financing. The OMLP is also responsible for the dissemination of the results of its analyses to competent authorities. The disclosure requirements in the new APMLFT are provided in Art. 101 and are in line with this criterion.

314. *Criterion 29.2* - The OMLP serves as the central agency for the receipt of STRs and of additional information, including (a) data on cash transactions exceeding 15.000 EUR; (b) wire transfers exceeding 15.000 EUR if the receiving subject has its/his/her residence or seat in a country with higher ML/FT risk; (c) wire transfers exceeding 15.000 EUR if the assets are transferred to a financial institution in a country with higher ML/FT risk. The OMLP receives from the tax Authority data on any declared or undeclared import or export of cash amounting to or exceeding EUR 10,000 when entering or leaving the European Community (Art. 120 APMLFT).

315. The APMLFT (Art. 68 (4)) provides exceptions from CTR reporting for auditing firms, independent auditors, legal entities or natural persons when they perform accounting or tax advisory services. As per this article of the law, *the minister responsible for finance shall issue rules setting the conditions under which the obliged person shall not be required to forward to the Office the data on certain customer transactions referred to in paragraph 1 of this Article.*

316. *Criterion 29.3*

a) The OMLP is legally empowered to require additional data and information from the reporting entities (Art. 91 APMLFT), while Art. 92 regulates OMLP's power to request to a lawyer, law firm or notary the submission of data needed for detecting and proving money laundering, predicate criminal offences, and terrorist financing. In such request OMLP has to specify the data required, the

legal basis for submission, purpose of processing, and the time limit within which the required data should be made available to them.

b) The OMLP has access to a number of external information databases and any submission of data, information and documentation to the OMLP under the APMLFT is free of charge. Art. 87(4) states that the OMLP shall have timely, direct or indirect access to data, information and documentation which are at the disposal of obliged persons, state authorities and holders of public authorisations, including information relating to the detection and prosecution of criminal offences. Details on databases directly accessible by the OMLP are included in the Art. 136(6) APMLFT.

317. *Criterion 29.4*

a) The OMPL carries out operational analysis by using the information received from reporting entities and the other information available to it, (see c.29.3) in order to determine whether there are grounds to suspect money laundering, predicate offences and terrorist financing in relation to a transaction, person, property, or assets.

b) OMLP conducts research and analysis of trends and typologies of ML and FT. However, the last typologies research published on the OMLP website dates back to 2011. The annual report of the OMLP contains information on trends and patterns and a number of other documents which examine the strategic aspects of the AML/CFT system. Art. 120-122 APMLFT provide details on state authorities' and holders of public functions' obligations with respect to the provision of data to the OMLP for the purposes of strategic analysis.

318. *Criterion 29.5* - The OMLP can disseminate spontaneously information and the results of its analysis to competent authorities if it considers that there are grounds to suspect ML, related predicate offences, FT or other criminal offences (Art. 101 and 102 APMLFT). The OMLP can also disseminate information upon the reasoned request of a number of authorities (the Court, the prosecutor's Office, the police, the Financial Administration and the permanent coordination group established pursuant to the Act regulating restrictive measures) under Art. 116 to 118 APMLFT. None of these articles refers to the *dedicated, secured and protected channels for dissemination*, while Art. 122 (2) stipulates that i) *disclosures; ii) information requested by relevant authorities; iii) information on temporary suspension of a transaction; iv) information concerning ongoing monitoring of the customer's business operations; v) any other information concerning OMLP analysis; and vi) information on pre-trial investigation or criminal proceedings that have been, or are likely to be, launched against the customer or a third person on grounds of ML/FT* are to be treated according to their level of confidentiality, and in line with the requirements of the Act regulating classified information, thus securing their protection and confidentiality.

319. *Criterion 29.6*

a) Information is classified and treated according to their level of classification, in accordance with the Act regulating classified information. However, the classification can be lifted by the Head of the OMLP. The information exchange (in hard copies) between OMLP and Police concerning the disclosures on STRs is classified under the one of four possible confidentiality levels – "INTERNO" (Restricted), "ZAUPNO" (Confidential), "TAJNO" (Secret) and "STROGO TAJNO" (TOP SECRET)[79].

b) All OMLP staff must have a security clearance up to a minimum level "for official use" since all received STRs are marked with this level of security. Nevertheless, every employee has to qualify and go through the security check for the "secret" level of security. The director of the OMLP has a "top secret" security clearance.

c) For security reasons the OMLP has its own servers and secured IT system. This system can be accessed only by OMLP staff with a password and each STR can be accessed only by a designated employee, the Head of STR Sector and the Director. The premises of the OMLP are occupied

[79] Art. 10 and 13 Act regulating classified data.

exclusively by the OMLP staff and are protected physically and electronically. Access to the information system is password protected.

320. *Criterion 29.7*

a) There are no legislative obstacles which would impede the OMLP from carrying out its functions in line with this criterion. Art. 87(3) APMLFT specifically stipulates that the OMLP is fully autonomous, self-standing and operationally independent in carrying out its responsibilities, including analysing data, information and documentation as well as disseminating the results of its analysis to the competent authorities.

b) The provisions of the Art. 103 APMLFT stipulate that international cooperation shall be carried out accordance with this Law (including the independence requirements) unless otherwise stipulated by international agreements. In order to achieve strategic and operational goals the OMLP and domestic authorities may conclude Memoranda of Understanding and may establish Inter-Departmental working groups (Art. 7 APMLFT). MoUs are, on behalf of OMLP, signed by its director.

c) The OMLP is a constitutive body of the Ministry of Finance, however, it is physically and functionally separated from the ministry. As per the new law, the OMLP is *entirely autonomous and operationally independent*. Its role and duties are stipulated in the Chapter VI of the AML/CFT law (Art. 87-119).

d) The OMLP has its own budget, which enables it to work independently. The OMLP submits its budget to the Ministry of Finance which is a decision making authority in this matter. However, the assessment team was informed that the OMLP does not have specific regulations on recruitment procedures. The annual budget of the OMLP is approximately 700.000 EUR; it is expected to be increased in 2017.

321. *Criterion 29.8* - As stated in the 4th round MER (par. 127) The OMLP is a founding member of the Egmont Group, thus it actively participates in its activities and cooperates with other Egmont Member FIUs since 1996.

Weighting and Conclusion

322. All criteria are met. **Slovenia is rated C with R.29.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

323. In its 4th MER Slovenia was assessed as partially compliant on the requirements that now fall under R.30. The deficiencies identified were related to the low level of ML investigations. It was also noted that insufficient priority was given to the recovery of assets, the detection and the investigation of fund-generating crimes by law enforcement agencies, prosecution and other competent authorities.

324. *Criterion 30.1* - The Police is an independent body, located within the Ministry of Interior, performing its tasks at three levels - state, regional and local (respectively, by the General Police Directorate, the Police Directorates and the police stations). The Financial Crime and Money Laundering Section (FCMLS) is a specialised unit responsible for combating financial crime and ML at the state level and is a part of the Economic Crime Division of the Criminal Police Directorate at the General Police Directorate. In addition, it oversees, coordinates, analyses and supervises the work of the police directorates in charge of combating financial crime (including ML). The FCMLS has five employees. It cooperates with institutions and state bodies at the national level, international organisations and foreign security bodies. In 2010 the National Bureau of Investigation (NBI) was established within the General Police Directorate. It is a specialised criminal investigation unit for the detection and investigation of more complex cases of economic, financial and organised crime. The criteria determining cases investigated by the NBI are regulated by the *Instructions on the Type of Criminal Offences to be Investigated by the NBI*, approved by the Director General of Police. Irrespective of the criteria provided by the Instructions, the NBI may initiate or undertake an investigation upon written request by the Specialised State Prosecutor's Office, the head of an

individual District State Prosecutor's Office or heads of different state authorities (Art. 22(2) Police Organisation and Work Act). Further to this, Instructions on types of offences the investigation of which is to be performed by the NBI underlines the complex cases of economic crime, corruption, organised and other types of criminality which generate high amounts of proceeds and when cross-border and inter-institutional cooperation, involving specific expertise, is needed when investigating them. Authorities also advised that terrorism financing could be a subject to NBI's investigations as per the above referred Instruction.

325. The Catalogue of Criminal Offences and Events, an internal act issued by the Director General, determines the offences and events dealt by the criminal police divisions of the police directorate. The investigations on ML are carried out by criminal police divisions of police directorates; and, exceptionally, by police stations.

326. There is no separate organisational unit designated for FT investigations. The Counterterrorism and Extreme Violence Section (CEVS) is a specialised police unit responsible for fight against terrorism. Although FT is not specifically mentioned within its competences, in practice, CEVS is also in charge to investigate FT.

327. In line with CPC, criminal investigations are led and supervised by prosecutors. Prosecutor also leads and supervises the activities of the special investigative teams. In 2011, Specialised State Prosecutor's Office of the Republic of Slovenia was set up, and is in charge to investigate and prosecute *serious criminal offences against the economy, offences subject to punishment of minimum ten years of imprisonment when the offence is committed by a criminal group; criminal offences involving corruption, terrorism, slavery relations and human trafficking*. Criminal offences regarding terrorist activities, which include the FT, are dealt under the general criminal department of the Special Prosecutor's Office.

328. *Criterion 30.2 -* The financial investigation is undertaken by the investigator dealing with the proceeds-generating crime and may be supported by a network of financial experts. Art. 499 CPC imposes *ex officio* financial investigations ('proceeds gained through the commission of a criminal offence or by reason of the commission thereof shall be determined in criminal proceedings'). Guidelines have been issued to ensure that parallel financial investigations take place.

329. Authorities also advised that the confiscation in criminal proceedings could only include the proceeds generated through the criminal offence(s) for which a conviction has been reached (Art. 507(2) and Art. 74 - 77 CC).

330. As for the requirement to carry out financial investigations *regardless of where the predicate offence occurred* the Act on Forfeiture of Assets of Illegal Origin enables competent authorities (prosecution) to initiate financial investigations whenever there are grounds to believe that property derived from crime. The Act lays down the '*terms and conditions, the procedure and the responsible authorities for financial investigation, the provision of temporary security of the forfeited assets, the secure storage, management and forfeiture of assets of illegal origin, the responsibilities of the Republic of Slovenia, and the manner in which international cooperation is to be carried out.*' The Act, which sets these investigations and proceedings into the civil law framework, also provides a catalogue of criminal offences that generate illegal assets. The catalogue includes, inter alia, ML and FT offences. In view of this it could be concluded that Slovenian legal framework enables to launch financial investigations regardless of where the predicate offence occurred.

331. *Criterion 30.3* - The police use financial investigations to identify the type and amount of proceeds, the assets that can be confiscated from holders of the proceeds, and the conditions required for the temporary securing of the assets concerned.

332. The legal basis for the conduct of financial investigations by the police is provided indirectly through Art. 499 and 507 CPC which stipulate that *evidence is to be gathered and circumstances material to the determination of proceeds are to be investigated during the pre-trial criminal procedure*. The same provision also appears in Art. 4 of the Police Tasks and Powers Act. Financial investigations can also be carried out by the special investigative teams set in line with Art. 160a CPC

and the related Decree *on the cooperation of the State Prosecutor's office, the police and other competent State bodies and institutions in detecting and prosecuting the perpetrators of criminal offences and on the operation of specialised and joint investigation teams*. The authorities confirmed that the confiscation in criminal proceedings can only cover the proceeds generated by the criminal offence(s) for which the conviction was secured. Thus, so called 'extended confiscation' *which would look into the property which did not derive from the crime actually investigated, but was likely of illegal origin*, is not possible. The latter is compensated by the introduction of the Forfeiture of Assets of Illegal Origin Act (FAIOA) which provides the police with the following competences:

- to propose to the prosecutor to instigate a financial investigation with stated reasons for suspicion (the second paragraph of Art. 10);
- to implement tasks (Art. 11 and 12) according to the instructions of the state prosecutor after the financial investigation was ordered by the State Prosecutor's Office.

333. Art. 14 FAIOA calls for establishing of financial investigation teams headed by the prosecutor and composed of police, the representatives of FARS, OMLP, SMA and the Slovenian Competition Protection Agency and the Court of Audit of the Republic of Slovenia. If the prosecutor requests an order for the temporary security or temporary forfeiture of assets or an extension of these measures, the court shall decide on such request within eight business days of receipt (Art. 21 - 24 and 28).

334. *Criterion 30.4* - Slovenia does not have competent authorities which are not LEAs but , pursue, nonetheless, financial investigations of predicate offences.

335. *Criterion 30.5* - There is no dedicated competent authority for the investigation of criminal offences related to corruption. The Commission for the Prevention of Corruption (CpC) (regulated by the Integrity and Prevention of Corruption Act) is an administrative authority which conducts administrative investigations on allegations of corruption, conflicts of interest, illegal lobbying and other violations of due conduct. The investigation of criminal offences (and recovery of assets gained thereof), including those of ML and funds-generating crimes, is the responsibility of the police and the State prosecutor's office. In these cases, the CpC can only provide information to the police or the State Prosecutor's office and provide assistance, for example, in joint investigation teams.

Weighting and Conclusion

336. All 5 criterions are met. **Slovenia is rated C with R. 30.**

Recommendation 31 - Powers of law enforcement and investigative authorities

337. Slovenia was rated Compliant with regard to R.28. The applicable law has changed, so the new analysis has been undertaken.

338. *Criterion 31.1* - The prosecutor is *dominus litis in criminal investigations* with powers to direct and supervise the police in this process.

a) Under Art.156 of the CPC, the investigative judge may order a bank, savings bank, payment institution or an electronic money company to disclose the information and documentation on deposits, statement of account and account or other transactions by the suspect, the accused and other persons who may reasonably be presumed to have been implicated in the financial transactions or deals of the suspect or the accused, if such data might represent evidence in criminal proceedings or is necessary for the confiscation of objects or securing of a request for the confiscation of proceeds or property in the value of proceeds. This measure cannot be applied to DNFBPs nor other "natural or legal person" and does not apply to the production of all records.80 In

[80] During the on-site visit, Slovenian authorities indicated that similar measure could be applied to DNFBPs and referred to Art. 150 of the CPC. However, the provision of the Article allows the control of the computer systems of banks or other legal entities which perform financial or other commercial activities and not of DNFBPs.

some specific instances (if there are reasonable grounds to suspect that the criminal offence for which a perpetrator is being prosecuted ex officio has been committed or is being prepared) the police may, through a written request, order the bank, savings bank, payment institution or the electronic money company to provide information without delay. In addition, Article 148 of the CPC provides that (1) If grounds exist for suspicion that a criminal offence liable to public prosecution has been committed, the police must take steps to discover the perpetrator, (…) detect and preserve traces of crime or objects of value as evidence, and collect all information which may be useful for the criminal proceedings(2) to this end, the police may: seek information from citizens; (…) perform actions which are necessary to identify persons and objects; send out a wanted circular for persons and objects; inspect in the presence of the responsible person specific facilities, premises and documents of enterprises and other legal entities, and undertake other measures necessary (…). This specific provision, although wide in its scope, has been used by the authorities to perform the actions foreseen under this sub-criterion.

b) Search of persons and premises are provided under Article 214 CPC. A house and/or personal search may be conducted if justified grounds exist for the suspicion that a particular person has committed a criminal offence and there is likelihood of apprehending the accused during the search or of discovering any traces of the crime or objects of importance for criminal procedure (Art. 214 CPC). A search shall be ordered by court in the form of a warrant (Art. 215 (1) CPC). Under specific conditions (e.g. if someone is calling for help, if a perpetrator is caught in the act of committing a criminal offence is to be apprehended, if the safety of people or property so requires, etc.) both a house and a personal search may be conducted without a judicial warrant (Art. 218 (1) and (4) CPC).

c) Article 234 CPC provides the possibility of taking witness statements – those likely to give some information about the criminal offence, the perpetrator and other material circumstances shall be summoned as witnesses. This also includes the injured party, the injured party acting as prosecutor and the private prosecutor. The Code stipulates that 'any person summoned as a witness shall abide by the summons'.

d) The confiscation of objects can be conducted independently or in the context of other investigative measures such as house or personal search. The objects may be confiscated by the police during the pre-trial procedure on the basis of their powers (Art. 148(2), 164(1) and 218(1) CPC). During the main hearings such a request can be issued by the court. The written order shall only be issued if the court requires a certain person to hand over the objects. If the court issues an order for a house search or personal search, it shall also include the powers (order) for the seizure of objects. The seizure of objects is of a temporary nature, and concerns the instrumentalities to commit the offence (corpus delicti) and evidence.

339. *Criterion 31.2* - The CPC provides competent authorities with a wide range of special investigative techniques and methods. Some special investigative methods which concern cooperation with the EU Member States when investigating international criminal activities, are also regulated under the Act on International Co-operation in Criminal Matters between the Member States of the European Union (ACCMEU).

340. Special investigative techniques are regulated by Articles 149a to 155a and Art. 156a CPC - they include secret surveillance (Art. 149a), obtaining information on communications using the electronic communications networks (Art. 149b), monitoring electronic communications *(sub-criterion b)* – Art. 150, control of letters and other parcels, control of the computer systems (sub-*criterion c)* of banks or other legal entities which perform financial or other commercial activities (Art. 150(3)), and listening to and recording conversations, listening and surveillance in another person's home or in other areas (Art. 150(4)). Use of undercover agents/undercover operations (sub-*criterion a*) is regulated by Art. 155a and covers wide range of measures to be used in such operations. However, controlled delivery (sub-*criterion d*) is not specifically regulated under the CPC. Some of its elements are included in Art. 155, nevertheless they only concern feigned purchase, the feigned acceptance or giving of gifts and the feigned acceptance or giving bribes. The Article does not refer to the possibility of LEAs to order controlled delivery under their supervision, which would

be executed/delivered in the territory of Slovenia, or would enter, transit through and exist from it. The latter would include cooperation with the jurisdictions involved in the investigation.

341. The above-mentioned investigative means can also be used in relation to the criminal offences of money laundering and terrorist financing (except for listening and surveillance in another person's home or in other areas with the use of technical means and, where necessary, secret entrance into the aforementioned home or area which can be used only if the criminal offence of money laundering was committed within a criminal association for the commission of such offence).

342. *Criterion 31.3* - In line with what was elaborated under c.31.1, the CPC (Art. 156) provides the possibility to access financial data and to carry out the secret monitoring of financial transactions upon the investigative judge's approval and on prosecutor's request.

a) Slovenia has a special register of bank accounts managed by the APLRRS (Art 143 – 148 PSSA). The register gathers information on transaction accounts and holders of the accounts of legal and natural persons. This Register contains all the necessary information required under c.31.3 a). The police can access the Register on the basis of the Agreement on the Direct Electronic Access to Information on the Transaction Accounts of Natural Persons from the Register of Transaction Accounts via the back-office application signed between the APLRRS and Police on 31 January 2011. The access to information on transaction accounts of legal persons is public and, therefore, also available to police.

b) The banks, savings banks, payment institutions or electronic money companies, once ordered to disclose information and send documentation which concern the suspect/accused, must not disclose to their clients or third persons that they have done so, or that they intend to send such information/documentation to the investigating judge (Art. 156(6) CPC).

343. *Criterion 31.4* - Art. 116, Para 1 APMLTT stipulates that the OMLP shall submit to the court, prosecutor's office or police, upon its written and reasoned request, the data from the records referred to in points 1 – 5 and 9 – 12 of Art. 136(4) of this law, which the court or prosecutor's office need for the purposes of investigating ML/FT and predicate offence circumstances vital for the protection or forfeiture of proceeds. In addition, Agreement on Mutual Cooperation in the Field of the Detection and Prevention of Money Laundering and Terrorist Financing signed between the Slovenian Police and the OMLP ensures coordination of actions of both institutions thus also preventing the duplication of investigating actions.

Weighting and Conclusion

344. The powers of law enforcement authorities to conduct ML, associated predicate offences and FT investigations including the application of compulsory measures and special investigative techniques are in line with criteria 31.1 to 31.3. Nonetheless, criterion 31.2 is largely met as there are limitations in the regulation of controlled delivery. **Slovenia is rated LC with R. 31.**

Recommendation 32 – Cash Couriers

345. Slovenia was rated compliant with respect to SR.IX on the cross-border transportation of currency and other financial instruments during the 3rd round in 2005.

346. *Criterion 32.1* - As a member of the EU, Slovenia is also bound by the EU legislation (the EU Regulation 1889/2005/EC). A declaration system for incoming and outgoing cross-border transportation of currency and bearer negotiable instruments (BNIs) is regulated by FEA (Art. 14). A declaration is required for all physical cross-border transportation, whether by travellers or through mail and cargo. However, this declaration system applies only to movements (both inward and outward) of cash and BNI from and to the EU, thus only movements that cross the external borders of the EU are subject to the declaration requirements. Movements of cash and BNI within the EU are not considered to be cross-border movements under the Foreign Exchange Act and are not subject to any declaration/disclosure obligation.

347. *Criterion 32.2* - Slovenia has established a written declaration system for all persons carrying cash or bearer-negotiable instruments (BNIs) equal or above a pre-set threshold of 10.000 EUR. The definition of cash is set out in the first paragraph of Art. 3 FEA. The Slovenian declaration form includes information on declaring person (including full name, date and place of birth, and nationality), the owner of cash, the intended recipient of cash, the amount and nature of cash, the origin and intended use of cash, the transport route and the means of transport.

348. *Criterion 32.3* - This criterion is not applicable since Slovenia has a declaration system.

349. *Criterion 32.4)* - Art. 14 FEA provides customs authorities with abilities to conduct supervision of the nature and quantity of cash transported into or out of the Community (EU) by residents and non-residents. In line with Art. 3 of the EU Regulation 1889/2005/EC obligation to declare is not fulfilled until the information provided is correct and complete. Thus, the customs authorities may request additional information (including via a standardised declaration form) from the traveller with regard to the origin of the currency or BNI and their intended use for the purposes of compliance with the obligation to declare.

350. *Criterion 32.5* - The FEA in its Art. 16 and 17 provide administrative sanctions for breaching the provisions related to false declaration. As stated above, such sanctions can be imposed by the customs administration. The level of these administrative sanctions varies between 500 EUR and 42.000 EUR (for legal entities). A fine might also be imposed to the responsible person of the legal entity. Art. 14 FEA regulates sanctions in case of failure to declare cash - the customs authority shall seize an entire consignment of undeclared cash if it amounts to EUR 10.000 or more, including the means of transport as specified in Art. 17 FEA. Those sanctions appear to be dissuasive and proportionate.

351. *Criterion 32.6* - Art. 120 APMLFT is setting an obligation for the customs authorities to forward to the OMLP, within three days' time, the data on any declared import or export of cash (from and to the EU) amounting to or exceeding EUR 10,000. The customs authorities are obliged to provide such data even if the import or export of cash was not declared to the customs authorities and if, in connection with the person who carries the cash, the manner of carrying or other circumstances thereof provide grounds to suspect ML or FT.

352. *Criterion 32.7* - Domestic coordination concerning the cross-border currency controls provides customs administration with a possibility to consult Police, and if the customs possess some additional information, send it as a notification on potential criminal activity in accordance with Art. 145 CPC. Cooperation between the customs administration and police has been formalised through the cooperation agreement signed on 15 March 2016. Art. 3 of this agreement stipulates that the two institutions can share and exchange data and information, organise joint working meetings, plan activities and execute joint actions, set contact points, provide technical support, expertise, analysis, joint trainings and best practises, as well as preventive activities. Furthermore, they also signed a protocol on submission of information and data sharing and a protocol on cooperation in training.

353. *Criterion 32.8* - The Slovenian legislation does not explicitly provide the Customs administration with the abilities to freeze or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/FT exist. Theoretically, police can – in case of suspicion of ML/FT or predicate offence or in any other suspicion of criminal activity – seize currency in accordance with the provisions of Art. 220 CPC (Seizure of objects). This Article provides for seizure of objects which must be seized as per the CC provisions, or which may be used as evidence in criminal proceedings. As underlined under c.32.7 above, the customs authorities have the possibility to consult the Police or Prosecutor's Office, including by way of sending a notification on potential criminal activity based on Art. 145 CPC.

354. With regard to the requirements of c.32.8 b) the evaluation team can accept that Art. 17 Foreign Exchange Act provides legal basis, but only to a certain extent and in a general manner.

355. *Criterion 32.9* - The general requirement for exchange of information among EU countries and with third countries is regulated by Art. 6 and 7 of the Regulation 1889/2005/EC. This Regulation is

implemented by the Slovenian customs administration. Moreover, Art. 103 - 107 APMLFT provide the modalities for the information exchange related to ML and FT internationally, including information on declaration. As a member of the EU, Slovenia also applies EC Regulation No. 515/97 on mutual assistance in customs matters.

356. *Criterion 32.10* - As a member of the EU, Slovenia respects the EU's principle of free movement of capital. Furthermore, the Preamble 1 of the Regulation 1889/2005 states that the European Community endeavours to create a space without internal borders in which the free movement of goods, persons, services, and capital is ensured. Personal data privacy is ensured by Art. 8 of the Regulation 1889/2005/EC. Any disclosure or communication of information shall fully comply with prevailing data protection provisions, and more precisely of the Regulation (EC) 45/2001.

357. *Criterion 32.11* - Individuals who are carrying out a physical cross-border transportation of currency or BNIs that are related to ML/FT or a predicate offense, could be subjects to criminal sanctions, as foreseen by the Art. 73 to 77.c CC and Art. 502 to 502.e CPC. As for seizure/confiscation of currency or BNIs – Art. 245 and 109 CC and Art. 491 to 507 CPC regulate this matter.

Weighting and Conclusion

358. The regime on cross-border transportation of currency and other financial instruments is in line with the standards, with the exception of Criterion 32.1, whereby the declaration system does not apply to movements of BNI and cash within the EU. Furthermore, as concerns Criterion 32.8, the Customs administration does not have the power to freeze or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/FT exist. **Slovenia is rated PC with R. 32.**

Recommendation 33 – Statistics

359. Slovenia was rated largely compliant with regard to the former R. 32. The bases for the rating were mainly related to the lack of statistics in number of areas.

Criterion 33.1 - Slovenia maintains statistics regarding the following areas:

a) Art. 114(5) APMLFT states that OMLP '*collects and publishes statistical data on money laundering and terrorist financing'* while Art. 133-135 regulate the type of data OMLP shall collect and make available for purposes of preparing of the NRA (Art. 133) which includes number of STRs received and disseminated. The same Article also sets an obligation that the annual statistics are sent to the European Commission on regular basis.

b) OMLP keeps statistics on every investigation, prosecution and conviction related to ML/FT (Art. 134 APMLFT);

360. It needs to be noted that, apart from OMLP, LEAs and courts also keep statistics in this matter. However, the methodology of data collection/statistics differs significantly among these institutions. Therefore, thorough analysis based on statistics and information provided by different institutions, in this context, might not be possible.

361. Art. 134 (1) point 7 APMLFT also requires OMLP to gather annual statistics on value of secured, confiscated, or seized illegal assets in euros. Furthermore, Art. 206 of the State Prosecutor's Office Act, foresees that the Expert and Legal Information Centre (ELIC) as a specialised expert body of the prosecution, keeps statistics on temporary seized and finally confiscated property gained from the criminal offences. The central statistics is managed on the basis of data, which are forwarded by all state prosecutors' offices immediately after the seizure/confiscation order, direction or other procedural act is issued, and also once the court order in this matter is available.

362. Since 1 January, 2016 the MoJ gathers data regarding requests for international co-operation with respect to extradition and mutual legal assistance. The MoJ therefore keeps statistics on number of requests made, received, processed, granted, or refused, types of request, etc. However, the legal basis to which the authorities referred (Chapter 30 CPC) does not impose on the MoJ any

obligation to keep statistics on MLA. OMLP keeps statistics on every MLA sent or received on the basis of the Council of Europe Conventions 141 and 198.

Weighting and Conclusion

363. Slovenia meets the criterion of this recommendation, however, the legislation does not explicitly impose the MoJ any obligation to keep statistics on MLA. **Slovenia is rated LC with R. 33.**

Recommendation 34 – Guidance and feedback

364. In the 4th round evaluation Slovenia was rated largely compliant with the former R.25 and it was stated in the report that more industry specific guidelines are required as well as guidelines on FT.

365. *Criterion 34.1* - According to Art. 154 APMLFT the supervisors and other competent authorities are required to issue guidelines regarding the implementation of the law. Guidelines have been issued by all competent authorities or the OMLP and they are specific for the industry for which they were prepared. The guidance documents include indicators for suspicious transactions.

Weighting and Conclusion

366. **Slovenia is rated C with R.34**

Recommendation 35 – Sanctions

367. In the 4th round evaluation Slovenia was rated partly compliant with the previous R.17 on the grounds of effectiveness issues.

368. *Criterion 35.1* - Chapter X APMLFT prescribes the fines that can be imposed for violations of the law by the respective supervisory bodies which are defined in the APMLFT (Art. 139).

369. The levels of fines depend on the seriousness of the offence in accordance to the list included in Art. 163 to 165 APMLFT. The levels of fines, in EUR, are as follows:

	Particularly grave offences committed by FI or Credit institution	**Particularly Grave offences**	**Gravest offences**	**Grave Offences**	**Minor Offences**
Legal Person/Law firms/Notaries	Up to 5,000,000 or 10% of turnover*	Up to 1,000,000	12 000 to 120 000	6 000 to 60 000	3 000 to 30 000
Responsible person of legal entity*	Up to 500,000 or 10% of turnover*	Up to 250,000	800 to 4 000	400 to 2 000	200 to 1 000
Sole proprietor/Self employed	Up to 2,500,000 or 10% of turnover*	Up to 500,000	4 000 to 40 000	2 000 to 20 000	1 000 to 10 000

*** The highest of the two

370. According to the provisions stipulated by Art. 139 APMLFT all supervising bodies, in exercising supervision, have the right and duty to:

1. Order measures to remedy the irregularities and deficiencies within the time limit as specified by it;

2. Carry out proceedings in accordance with the law regulating minor offences;

3. Propose the adoption of appropriate measures to the competent authority if it is relevant for another authority

4. Order other measures and perform acts for which it is authorised by law or any other regulation.

371. According to the Art. 139 APMLFT in conjunction with provisions of the BA (Art. 249 and 250), BoS has power to impose supervisory measures such as order to eliminate violations (Section 8.3.1); early intervention measures (Section 8.3.2); and withdrawal of authorisation to provide banking services (Section 8.3.3). In addition to that the BoS can take supervisory measures against qualifying holders (Section 8.4) and a member of the governing body (Section 8.5). The measures listed in Section 8.3 BA are intended for prudential supervision but they can be used for AML/CFT purposes as well. Similar measures can be imposed on payment service providers in accordance with Chapter 13 of the PSSA.

372. In most cases an Order to eliminate violations is used in order to inform the obliged entity about the nature of detected violations and to impose them an obligation to eliminate the violations within the defined deadline. In the case when identified violations are not severe a Supervisory letter is used.

373. In addition to the above, Art. 161 APMLFT obliges competent authorities to disclose the information on AML/CFT violations by publishing them on their web site.

374. According to Art. 302 (1) IA, ISA can issue an order to eliminate violations or irregularities or to perform or omit action relating to verifying the legality of their operations and in particular rules in the act. This is interpreted to give the ISA powers of sanctioning AML/CFT violations as well.

375. The SMA under FIMA can impose sanctions on all types of violations and this applies both to legal and natural persons (art. 556 to 572) and can include AML/CTF violations.

376. In accordance with Art. 81 Auditing Act, APOA has power to sanction audit firms, certified auditors and the management of audit firms in case of violation of relevant legislation referring to audit firms, Sanctions can also be imposed on AML/CFT violations as the auditing rules include "other laws governing the auditing of individual legal entities" (art. 4) The possible sanctions are; an order to rectify violations, a reprimand, or to conditionally withdraw a licence or withdraw a licence.

377. *Criterion 35.2* - As mentioned in c.35.1, BoS, ISA, SMA, FMA and APOA can also sanction natural persons which include directors and senior management. According the Article 163 of the APMLTF administrative sanctions (fines) might be imposed to natural persons as well regardless the type of supervisory authority.

Weighting and Conclusion

378. Both criteria are met. **Slovenia is rated C with R.35.**

Recommendation 36 – International instruments

379. In the 2010 MER, Slovenia was rated largely compliant with the previous R.35 and SR.I. The confiscation provisions, especially from the Palermo Convention but also from the Vienna Convention, were not fully implemented in order to have a strong confiscation regime. Additionally, there were reservations about full implementation of the regulatory and supervisory regime for bodies other than FIs susceptible to ML under the Palermo Convention.

380. *Criterion 36.1* - Slovenia is party to all four Conventions listed in the standard. Slovenia notified succession to the Vienna Convention in 1992, ratified the Palermo Convention and the FT Convention in 2004 and the Merida Convention in 2008.

381. *Criterion 36.2* - This criterion requires the full implementation of a range of specified articles of the UN Conventions mentioned above. Slovenia has largely implemented the provisions of the Vienna, Palermo, Merida and FT Conventions into domestic law.

382. The level of implementation is however subject to the conclusions regarding the minor shortcomings in R.3 which are relevant for Art. 3 Vienna Convention, Art. 6 Palermo Convention and Art. 23 and 28 Merida Convention. The minor deficiencies identified for R.4, which cascade on R.38, undermine the implementation of Art. 5(2) and (4) Vienna Convention, Art. 12(2) and 13 Palermo Convention, Art. 31 (2), 54 and 55 Merida Convention and Art. 8 (1) of the FT Convention as far as confiscation of instrumentalities is concerned and Art. 31 (3) Merida Convention in terms of management of confiscated assets. The deficiency described under R.5 regarding the application of a purposive element for the financing of FT Convention Annex offences, undermines the implementation of Art. 2(1)(a) and Art. 11 of the FT Convention.

383. Some gaps in legal powers for the investigative technique of controlled delivery as described under R.31 mean that Art. 11 Vienna Convention and Art. 50 Merida Convention are not fully implemented. The gaps in powers to prevent and detect cross-border movement of cash within the EU territory (see R.32) adversely impact on implementation of Art. 7(2) Palermo Convention, 14 (2) Merida Convention and 18 (2) FT Convention.

384. The evaluation team did not receive information to allow a conclusion as to whether the asset recovery requirements of Art. 14(2) Palermo Convention, Art. 8(4) FT Convention, and Art. 51 and 53 Merida Convention are implemented.

Weighting and Conclusion

385. Most provisions of the Vienna, Palermo, Merida and FT Conventions have been largely implemented in the Slovenian legal order. There are certain shortcomings with respect to R. 3, 4, 5, 31, 32, as a result of which not all provisions of the Conventions are fully implemented. **Slovenia is rated LC with R.36**.

Recommendation 37 - Mutual legal assistance

386. In the 2010 MER, Slovenia was rated largely compliant on the former R.36 and SR. V, because the lack of detailed statistics on cooperation relating to ML/FT or predicate offences undermined the assessment of effectiveness. Slovenia was rated compliant on the former R.37 (on dual criminality standards). The current version of R.37 consolidates the MLA aspects of all three former Recommendations mentioned above.

387. *Criterion 37.1* - Slovenia is a party to a range of international instruments relating to MLA, including the European Convention on Mutual Assistance in Criminal Matters of 1959 and its two additional Protocols and the 2005 Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (Warsaw Convention), as well as to several bilateral agreements. MLA is provided pursuant to Chapter 30 of the CPC unless provided otherwise by international agreements (Art. 514 CPC; principle of subsidiarity of the national legislation). The Act on Cooperation in Criminal Matters with the EU Member States (hereafter: ACCMEU) transposes into the legal order all adopted instruments of the EU on mutual recognition in criminal matters, relevant procedural provisions regarding MLA, transfer of proceedings, transfer of the execution of sentences and cooperation with EU entities such as Eurojust and European Judicial Network. Furthermore, it is also possible to provide MLA on the basis of the principle of reciprocity and national laws. Slovenia thus possesses a legal basis that allows it to provide a wide range of assistance in relation to investigations, prosecutions and related proceedings involving FT, ML, and associated predicate offences. The incomplete criminalisation of

FT (see R.5) and the minor gaps in the criminalisation of ML (see R.3) could however be an issue when responding to foreign requests for MLA in cases where dual criminality is required.

388. *Criterion 37.2* - According to the CPC (Art. 515), MLA requests are transmitted through diplomatic channels (MFA). In practice, requests are generally submitted directly through the MoJ on the basis of most bilateral as well as multilateral treaties which determine the MoJ as the central authority and enable communication through central authorities instead of diplomatic channels. The OMLP has been appointed as the central authority for handling MLA requests for the 1990 Strasbourg Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and the 2005 Warsaw Convention. In urgent cases and on condition of reciprocity, requests for legal assistance may be sent through the Ministry of Interior (responsible for the Police), or, in instances of ML or criminal offences connected to ML or FT, also through the OMLP (Art. 515 CPC).

389. In order to ensure the timely prioritization and execution of MLA requests, the MoJ uses an electronic case management system which sends out warnings when deadlines for the execution of requests have been reached. The OMLP also has a document managing system, which allows the registration and monitoring of requests that it has forwarded.

390. If reciprocity applies or if it is so determined by an international treaty, international legal aid in criminal matters may be exchanged directly between domestic and foreign bodies participating in the pre-trial proceedings and criminal proceedings (Art. 515(3) CPC). The ACCMEU enables direct communication between judicial authorities of EU Member States, in accordance with provisions of relevant multilateral instruments (such as Art. 6 of the 2000 Convention on Mutual Assistance in Criminal Matters between the Member States of the EU and Art. 53 of the Schengen Convention). The ACCMEU contains a general rule on prioritisation and expeditiousness of provision of legal assistance (Art. 5). In cases of direct communication (within or outside of the EU), the evaluation team was not informed about any case management systems in place for judicial authorities to monitor progress on requests.

391. *Criterion 37.3* - The provision of MLA is not subject to special conditions. Requests for MLA are executed in accordance with national legislation; however, the Slovenian authorities may also comply with the formalities and procedures expressly indicated by the requesting Member State, provided that such formalities and procedures are not contrary to the fundamental principles of the national criminal system (Art. 516 (4) and (5) CPC). MLA as prescribed by the CPC does not appear to be made subject to unreasonable or unduly restrictive conditions.

392. *Criterion 37.4* - The CPC and other relevant legislation do not prohibit the provision of MLA if the offence is also considered to involve fiscal matters. Secrecy or confidentiality requirements on FIs and DNFBPs are not grounds for refusal for MLA and can be lifted by court order as a general matter of law. See also under R.9 as far as FIs are concerned.

393. *Criterion 37.5* - Relevant international agreements to which Slovenia is a party and which are in force by virtue of Art. 514 CPC and Art. 8 of the Constitution contain provisions requiring to maintain the confidentiality of MLA requests. In other circumstances the authorities are of the view that Art. 128 and 188 CPC and Art. 201 of the Court Order provide the necessary protection.

394. *Criterion 37.6* - The dual criminality principle is not applied in relation to EU member states (under the Convention Implementing the Schengen Agreement, and the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU; Art. 49 ACCMEU). As concerns MLA requests originating from non-EU States, Slovenia has maintained the condition of dual criminality in relation to measures that it considers coercive, such as search or seizure of property, under the 1959 European Convention, the 1990 Strasbourg Convention and the 2005 Warsaw Convention.

395. There are no domestic provisions which clarify whether dual criminality is a condition for rendering assistance to non-EU countries when a MLA request does not involving coercive actions. The authorities are of the view that there are no domestic provisions which would bar providing

assistance in such a case. According to Art. 516 (4) CPC, "the permissibility and the manner of performance of an act requested by a foreign body shall be decided by the competent national authority pursuant to domestic regulations and international agreements and the request for international criminal assistance may be granted if the implementation of the act of assistance is not in conflict with the legal order of the Republic of Slovenia and does not prejudice its sovereignty and security". An absence of dual criminality does not mean per se that the execution of a non-coercive measure is in conflict with the legal order. The competent court would decide on the matter depending on the circumstances in the concrete case.

396. *Criterion 37.7* - The requirement of dual criminality is deemed to be satisfied regardless of the offence categorization or denomination, provided that both countries criminalise the conduct underlying the offence. This principle is explicitly stated in several multilateral treaties to which Slovenia is a Party. The evaluation team was reassured during the on-site visit that judges would interpret broadly Art. 516 CPC and would not consider execution of a request a breach of the legal order in case of no exact consistency between the domestic and foreign laws.

397. *Criterion 37.8* - Although there are no explicit provisions which prescribe that all the powers granted by the CPC and other laws may be used in response to an MLA request, this can be inferred by Art. 516 (4) CPC which provides that "competent authorities decide upon the manner of implementation of an act requested by a foreign authority pursuant to international agreements and *national regulations"*. Slovenia can also provide assistance to other EU countries in controlled delivery (Art. 55 ACCMEU), even if this special investigative technique is not available to LEAs in pure domestic situations (see R.31).

Weighting and Conclusion

398. Slovenia mostly meets criteria 37.1 and 37.2 and meets all other criteria. Slovenia possesses a legal basis to provide a wide range of MLA in relation to investigations, prosecutions and related proceedings involving FT, ML and associated predicate offences. There are no case management systems in place to monitor progress on requests direct communication between judicial authorities. Gaps in the FT offence and minor gaps in the ML offence could negatively affect Slovenia's ability to provide MLA in cases where dual criminality is a condition for executing MLA requests. **Slovenia is rated LC with R.37.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

399. In the 3rd round, Slovenia was assessed largely compliant on the former R.38 due to the fact that no asset forfeiture fund was being considered. In the 2010 MER, Slovenia was not reassessed on R.38.

400. *Criterion 38.1* - The legal framework described under R.37 also applies to MLA in the field of freezing and confiscation. MLA for the purpose of freezing and confiscation with non-EU states is conducted under provisions of various treaties, including the 1990 and 2005 Council of Europe Conventions, or the CPC. The cooperation with competent authorities of the EU Member States is regulated in Chapters 20 and 22 of the ACCMEU, implementing *inter alia* the Council Framework Decision 2003/577/JHA on the execution in the EU of orders freezing property or evidence, and the Council Framework Decision 2005/212/JHA on confiscation of crime-related proceeds, instrumentalities and property. It must be noted that Art. 210 ACCMEU gives quite extensive mandatory grounds for refusal of confiscation on the basis of a decision of a competent authority of another Member State, which could form an obstacle to expeditious action in response to foreign requests within the EU.

401. Generally speaking, Slovenia has the authority to take appropriate action in response to requests by foreign countries to identify, arrest and confiscate proceeds from, instrumentalities used in or intended for use in ML, predicate offences or FT, and property of corresponding value. Minor deficiencies in provisional measures for instrumentalities (see R.4) could to some extent limit authorities' ability to respond to requests. Outside of the EU framework, gaps in the FT criminalisation (see R.5) narrow Slovenia's powers to search and seize upon foreign request assets

used in FT activity since dual criminality is required for execution of such coercive measures in criminal proceedings.

402. *Criterion 38.2* - Authorities advised that Slovenia may provide assistance to requests for cooperation made on the basis of non-conviction-based confiscation proceedings in accordance with international agreements or EU legal acts which are directly applicable in Slovenia. If there are no such international legal bases or if they do not resolve any open issues, this assistance will be provided within the meaning of the provisions of Ar. 48-54 FAIOA. Assistance shall be provided under the conditions that the requested measure shall not be contrary to the fundamental principles of the domestic legal order; that its implementation shall not harm the sovereignty, legal order or other interests of Slovenia, and that the requesting country proves that it applies the standards of fair trial to asset forfeiture proceedings conducted in that country.

403. *Criterion 38.3* - (a) Slovenia does not have explicit legal arrangements for co-ordinating seizure and confiscation actions with other countries. Relevant provisions of CPC and FAIOA could apply in practice, since it appears that coordination could be arranged on a case-by-case basis, when authorities receive and implement a request for seizure and confiscation. Furthermore, the Expert Information Centre (EIC), a unit within the Office of the State Prosecutor General, has a coordinating and facilitating role in cooperation with EU Member States for the purpose of confiscation. It keeps a central register of all proposals and orders related to confiscation, provides expert assistance to State Prosecutors on the matter, and operates as the contact point between domestic and foreign competent authorities.

(b) Slovenia has basic mechanisms in place to manage and, where necessary, dispose of property frozen, seized, or confiscated, but it does not have sufficient procedures to deal with complex corporate assets, as described under R.4.

404. *Criterion 38.4* - Art. 216 ACCMEU provides a legal basis for sharing confiscated property with EU Member States. There are no domestic legal provisions or administrative procedures or processes which directly address the sharing of confiscated property with non-EU countries. Some of the relevant multilateral international agreements to which Slovenia is a party contain provisions on asset-sharing, which have force in Slovenian law by virtue of Art. 514 CPC and Art. 8 of the Constitution. Some of the bilateral agreements signed by Slovenia also contain provisions on asset-sharing. In other circumstances the Slovenian authorities are of the view that their legal framework would not prevent them from sharing confiscated assets on an ad-hoc basis, should the need arise.

Weighting and Conclusion

405. The Slovenian provisional measures and confiscation regime is generally comprehensive, allowing execution of MLA requests related to both criminal and civil based confiscation proceedings. Deficiencies identified under R. 3, 4 and 5 could to some extent limit the cooperation that can be provided. **Slovenia is rated LC with R.38.**

Recommendation 39 – Extradition

406. In the 3rd round MER, Slovenia was rated compliant on R. 39 (extradition for ML), R. 37 (dual criminality requirements in extradition procedures) and SR. V (extradition for FT). The 2010 4th round MER did not reassess Slovenia's compliance with R.37 and 39, and attributed a largely compliant rating to SR.V, on the basis of the incomplete criminalization of FT.

407. *Criterion 39.1* - The ACCMEU implements the 2002/584/JHA Framework Decision on the European arrest warrant and the surrender procedures between Member States. Extradition to non-EU Member States is governed by Chapter 31 CPC and relevant international instruments. Slovenia has ratified the Council of Europe Convention on Extradition in 1995 and its four additional protocols. Previously, aliens could only be extradited according to Art. 521(2) CPC in instances provided for by the international agreements binding on Slovenia, but this requirement was removed in 2011 through the Act Amending the CPC – K.

(a) ML and FT are extraditable offences.

(b) The extradition procedure for cooperation with non-EU Member States is elaborated in Art. 524-529 CPC with a decisive role for a panel of judges at the district courts. There is a general obligation on all bodies participating in criminal proceedings to proceed with special speed if the accused has been detained, which is usually the case in extradition procedures (Art. 200 CPC). The electronic case management system in the MoJ described under R.37 is also relevant for extradition requests and ensures prioritisation of consideration of extradition requests.

Part II of the ACCMEU provides for a clear surrender procedure to EU Member States with explicit provisions on the time limits and a general rule on prioritisation and expeditiousness. The ACCMEU also contains an explicit provision on the need to execute warrants or requests speedily and with priority if deprivation of liberty is ordered (Art. 80). There appear to be no case management systems in place for judicial authorities handling surrender requests through direct communication in the EU framework.

(c) Conditions on the execution of extradition requests are set in Art. 522 CPC and Art. 10-13 ACCMEU. Although quite extensive, the majority of them do not seem to be unreasonable or unduly restrictive. It must be noted however that Slovenia has incorporated many of the optional grounds as provided under the EU framework (Art. 4 of the 2002/584/JHA Framework Decision) as mandatory grounds for refusal of surrender in the ACCMEU (Art. 10), which restricts judicial discretion. Authorities advised that for cooperation with other State Parties to the European Convention on Extradition, certain requirements under the CPC which are not in line with the Convention, such as the need to establish of a *prima facie* case for extradition in the absence of a final judgment, do not apply due to the principle of subsidiarity of national law (Art. 8 Constitution, Art. 514 CPC).

408. *Criterion 39.2* - Extradition of Slovenian nationals to third countries is prohibited by Art. 47 of the Constitution. Under Art. 527 CPC as amended by the CPC-K in the event that the extradition is refused because the person is a Slovenian citizen, the extradition documents shall be handed over to the competent state prosecutor's office for the purpose of eventually instituting criminal prosecution in Slovenia. In accordance with Art. 20 CPC, the public prosecutor shall be bound to institute criminal prosecution if there is reasonable suspicion that a criminal offence liable to prosecution *ex officio* has been committed.

409. According to Art. 117 ACCMEU, Slovenian citizens may be surrendered to member states of the EU on the basis of the European Arrest Warrant. At the same time, if the warrant is issued for the purpose of executing a custodial sentence and the requested person is a Slovene national, there is an optional ground to refuse the surrender under Art. 11 ACCMEU. The conditions for this refusal are that the requested person declares that he or she wishes to serve the sentence in Slovenia, and that a national court undertakes to execute the sentence of the court of the ordering State in accordance with the national legislation, on condition that the circumstances exist which enable the execution of the sentence in Slovenia.

410. *Criterion 39.3* - Both the CPC (Art. 522 (3)) and the ACCMEU (Art. 9(1)) require the presence of dual criminality in order to extradite or surrender a person. Pursuant to Art. 9(2) ACCMEU, dual criminality shall however not be verified if a warrant is issued for a criminal offence punishable under the law of the ordering member state by deprivation of liberty for a maximum period of at least three years, and if such a criminal offence is classified under the law of the ordering state as one of the offence categories listed in Art. 2(2) of the Framework Decision, which include ML and do not include FT.

411. The law uses the formulation that the act for which the extradition or surrender is requested must be a criminal offence both within the meaning of domestic law and the law of the ordering country. Authorities have advised that this terminology is interpreted flexibly according to legal theory and by the courts, based on similar conduct irrespective of the terminology and formal qualification. In support of this assertion, they provided a decision of the Higher court in Ljubljana (Num. Kp 474/99 of 4 January 2000), stating that "refusal of extradition is only possible in case

when a particular *conduct* is not incriminated in accordance with the law of the Republic of Slovenia" (emphasis added). Previous assessments and the discussions during the on-site visit in the current round also confirmed that the condition of dual criminality is deemed satisfied if Slovenia also criminalises the conduct underlying the offence, irrespective of exact qualification. The gaps in the FT offence, which criminalises certain but not all FT conducts (see R.5), may however limit Slovenia's ability to provide extradition assistance. The gaps in the ML offence, which does not criminalise all conducts described under the Conventions (see R.3), may also limit possibilities to extradite to countries outside of the EU.

412. *Criterion 39.4* - Simplified extradition procedures are possible if the sought person consents (Art. 529a CPC; Art. 22 ACCMEU). Also, when there is a danger that the person sought might flee or go into hiding, the police can make an arrest upon petition by a foreign competent body, irrespective of how it was sent, if it is accompanied by a statement that extradition shall be requested by a regular route (Art. 525 CPC).

Weighting and Conclusion

413. Slovenia has appropriate extradition procedures. However, some weaknesses relating to the ML and FT offences may impact on the scope of application of these measures. **Slovenia is rated LC with R. 39.**

Recommendation 40 – Other forms of international cooperation

414. Slovenia was previously rated largely compliant on former R. 40, mainly due to lack of collection of detailed statistics which did not allow the evaluation team to form an opinion on the effective application of the legal framework.

415. *Criterion 40.1* - Competent Slovenian authorities can provide promptly a range of information to their foreign counterparts in relation to ML, predicate offences and FT. The OMLP can exchange - spontaneously and upon request – a wide range of information and cooperate with the foreign FIUs regardless of their status and based on reciprocity (Art. 89(7), 91 – 94, 104, 108 and 113 APMLFT). The same applies to the Slovenian police where authorities also noted that the membership in different international bodies (Interpol, Europol, Schengen area, SECI Centre – association of police and customs authorities of thirteen countries of South-East Europe, CARIN Group, etc.) to a large extent facilitates this cooperation. The Law on the Organisation and Work of Police (Art. 3 and 37) regulates the international cooperation issues and the role police have in it. Prosecutor's office (Art. 206 of the State Prosecutor's Office Act) and the relevant supervisory authorities (BoS, FARS; APOA) are also engaged in international cooperation.

416. *Criterion 40.2* - Competent authorities can exchange a wide range of data and information with their foreign counterparts on the basis of the following legal provisions.

a) Art. 103 to 108 APMLFT unless otherwise stipulated by international agreement(s). For the purpose of information exchange the OMLP may conclude Memoranda of Understanding with foreign FIUs. The chapter of the APMLFT referring to international cooperation also determines the conditions under which the OMLP can temporarily postpone a transaction on the basis of the initiative of the foreign FIU and *vice versa*. BoS cooperates with the competent authorities of other EU Member States, in particular by exchanging information which can facilitate supervision in accordance with the Articles 16 and 22 BA.

Under Articles 156 and 157 of APMLFT, all supervisory authorities can cooperate with foreign counterparts on issues related to the prevention of ML and FT, specifically with regard to the supervision of obliged persons and in order to facilitate supervision.

Cooperation with competent supervisory authorities from third countries is also regulated through bilateral Memoranda of Understanding. Art. 304 to 308 FIMA give SMA the legal basis for international co-operation. Information exchange is carried out in line with Article 488 and 488a FIMA, while cooperation with non-EU Member States is provided through IOSCO (International

Organisation of Securities Commissions) memorandum or bilateral MoUs signed. As concerns ISA, Article 289 IA regulates cooperation only with counterparts from other EU Member States. As far as EU members are concerned, cross-border police cooperation is carried out in line with the requirements of EU legislation. Co-operation in criminal matters between the competent Prosecutorial authorities of the Republic of Slovenia and foreign authorities is regulated by ACCMEU (adopted in 2013), under the CPA and based on Council of Europe Convention No. 198 since 2012.

b) There are no impediments that would prevent the competent authorities from using the most efficient means to cooperate.

c) The OMLP uses the IT secured channels of ESW and the FIU.Net. The same applies to Slovenian police (which is also member of the AMON network – Informal network for anti-money laundering and CARIN), the Prosecutor's office (including through CARIN, Eurojust, EJN – the European Judicial Network, the ARO platform and the AMO platform) and the relevant supervisory authorities. The APMLFT provides the legal basis for the OMLP to use secure communication channels for cooperation (Art. 112-113). However, no such legal requirements exist for other competent authorities.

d) The OMLP exchanges data on the basis of reciprocity in accordance with the provisions of the APMLFT. The exchange of information is done electronically through the above-mentioned protected channels. The SMA requests are made in writing and sent via facsimile, e-mail and regular post (privileged and confidential). The evaluation team was not provided with information with regard to the Insurance Supervision Agency and exchanges of information with EIOPA. The exchange of information between the Slovenian police authorities, as per Rules on Police Data Protection (2014) and their foreign counterparts is conducted through a secured connection, through encrypted security networks. The same applies to the Prosecutor's office[81] The prioritisation is made on case-by-case bases, as well as in accordance with the principles for information exchange provided in the international agreements (e.g. EGMONT standards) that the authorities comply with. No other internal guidelines or methodologies to assist the authorities in this matter were reported.

e) Most of the information exchange is processed in line with the law regulating classified information. However, some sectorial legislation is also applicable (such as Art. 488 and 488a FIMA).

417. *Criterion 40.3* - Under Articles 157 and 158 of the APMLFT all competent AML/CFT supervisory bodies listed in Article 139 can co-operate with foreign counterparts without the need to sign bilateral or multilateral agreements. The OMLP does not need to have a MoU in place in order to cooperate with other FIUs. Nevertheless, a number of memoranda have been signed.

418. In the course of a pre-trial proceedings, investigation or main hearings in one or more countries, the Police and State Prosecutors may also cooperate with the authorities of EU countries within the framework of a joint investigation team (JIT).

419. The State Prosecutor's Office does not require bilateral or multilateral agreements or arrangements to cooperate with foreign counterparts. International cooperation is based on criminal legislation (CPA, and Cooperation in Criminal Matters with the Member States of the European Union Act). Nevertheless, three bilateral agreements (memoranda) with non-EU members have been signed. The Slovenian police have signed numerous bilateral and multilateral agreements and protocols with a number of countries[82] strengthening common security interests and stepping up cooperation in combating cross-border crime.

[81] Art.117 of Police Tasks and Powers Act; Art. 1 and 14 of the Personal Data Protection Act; Art. 1 of the Classified Information Act; Art. 1, 10 11, 19 of the Rules on the protection of police data.

[82] Kosovo*, the Former Yugoslav Republic of Macedonia, Republic of Moldova, The Russian Federation, Republic of Croatia, USA, Ukraine, Republic of Serbia, Republic of Albania, Republic of Montenegro, Austria, France, Italy, Hungary.

420. *Criterion 40.4* - Under Article 109 APMLFT the OMLP forwards to the foreign FIU, upon its request and under the condition of effective reciprocity, feedback on usefulness and helpfulness of information received, as well as on the outcome of the analysis carried out based on the information received from the foreign FIU.

421. Police and ISA do not have a standard procedure for giving feedback to a foreign authority. This is rather done on case by case basis. Police provides feedback depending on the importance and urgency of the case. SMA is not required to do so by legislation and has never received a request for feedback from a counterpart. No information has been provided with regard to the other competent authorities.

422. *Criterion 40.5* - Provision of assistance by the relevant Slovenian authorities is not subject to unreasonable or unduly restrictive conditions. The only condition for an execution of assistance is that the content of the request does not conflict with the legal order of the Republic of Slovenia and does not to harm its sovereignty and security.

423. *Criterion 40.6* - Data submitted by the OMLP can be disclosed to the competent authorities of the country of the requesting FIU only when a prior consent of the OMLP is obtained (Art. 103 to 108 APMLFT). The OMLP can also forward data received from foreign counterparts to the competent Slovenian law enforcement authorities only when the prior consent of the foreign FIU has been received and for the purposes of detection and prevention of ML, FT and related predicate offences. Protection of police data is governed by Art. 118 – 130 of the Law on the Duties and Powers of the Police. However, in none of the paragraphs of these articles specific reference was made to the protection of data received from foreign police. With regard to prosecutors, Art. 180 of the State Prosecutor's Act stipulates that '*in implementing the cross-border exchange of data, the personal data shall be transmitted only to prosecution authorities or other similar authorities of other states or international organisations if required for the operation and/or decision-making of these authorities…. In cases when the third countries are involved, data may be transmitted only on the basis of an international agreement or in compliance with the decision of the national supervision authority for personal data protection pursuant to the provisions of the act regulating personal data protection.*'

424. The SMA can use the information exchanged only when exercising its supervisory competencies or tasks (Art. 488a (2) FIMA). The same applies to the ISA (Art. 290 and 509 IA). Art. 16(5) BA stipulates that the information exchanged might be used only for the purpose of supervision and should not be disclosed to third persons. No information has been provided with regard to other competent authorities.

425. Criterion 40.7 - This criterion is covered by the following provisions of the APMLFT – Art. 104(6) on guarantees needed when OMLP sends personal data to a foreign FIU; Art. 105 in cases when a foreign financial intelligence unit is requested by OMLP to submit data; and Art. 106(4) on situations when OMLP can refuse to fulfil the request submitted by a foreign financial intelligence (when guarantees regarding the data protection is in lacking, not satisfactory) and in Art. 106(6) which stipulates that OMLP shall give consent to a third persons to forward data with certain exceptions listed under this paragraph. State prosecutor must maintain as a secret (Art. 41 and 180 State Prosecutor's Act) the information obtained during the proceedings which concerns the clients and their legal and factual relations. Prosecutors shall protect the secrecy or confidentiality of all personal or other data that are not accessible to the public. This duty also applies to senior judicial advisors and other civil servants from the Prosecutor's offices. The Law on Duties and Powers of Police does not expressly provide for the protection of data received from foreign LEAs in the context of international cooperation

426. Art. 16 BA regulates this issue with regard to BoS. With regard to SMA, Art. 488 and 488a FIMA regulate this issue. No information has been provided with regard to other competent authorities.

427. *Criterions 40.8* - When a foreign FIU requests data, information and documentation, OMLP may use the whole range of its powers which it would normally use domestically (Art. 106 (2) APMLFT). The police may, if necessary, provide personal or other data to the authorities of third countries or

international organisations at their request or on its own motion subject to effective reciprocity (Art. 177 of the Law on the Duties and Powers of the Police). If a national judicial authority estimates, for well-founded reasons, that information obtained during the pre-trial proceedings or main hearing can be the subject of a request for legal assistance, it can forward this information to the competent authorities of another Member State without a prior request (Art. 52 ACCMEU). However, it remains unclear if and in which manner this can apply in cases which concern a non EU member state.

428. BoS can provide competent supervisory authority from EU Member States information which concerns supervision upon their request; it may also conduct inquiry on behalf of foreign counterparts; and conclude a cooperation agreement with the competent authorities of third countries with respect to the supervision of banks that provide services in a third country (Art. 22 BA).

429. The SMA can conduct inquires on behalf of foreign counterparts and, as appropriate, authorise or assist the foreign counterparts to conduct inquiries themselves in the country in order to facilitate effective group supervision. However, such possibility concerns only the EU Member States. No information has been provided with regard to other competent authorities.

430. *Criterion 40.9* - The legal basis for the OMLP to provide co-operation on money laundering and terrorist financing is set in Art. 104 to 108 APMLFT fully covering the requirements of this criterion.

431. *Criterion 40.10* - Please refer to text under c.40.4 – Art. 109 APMLFT fully reflects the requirements of this criterion.

432. *Criterion 40.11*

a) The OMLP has necessary powers to forward a request to a foreign FIU, and submit the data, information and documentation needed for detecting and preventing ML/FT. (Art. 105 and 106 APMLFT).

b) As already noted under c.40.8 when a foreign FIU requests data, information and documentation, the OMLP shall use the whole range of its available powers which it would normally use domestically on the basis of the new APMLFT (Art. 106 (2)).

433. *Criterion 40.12* - Please refer to text under c.40.2. Apart from that, no information has been provided in relation to FARS which supervises the implementation of the prohibition to accept payments for goods and performed services in cash in an amount exceeding €5,000.

434. *Criterion 40.13* - As per Art. 157 APMLFT, the OMLP and other supervisory bodies shall cooperate with bodies of third states which are competent for supervision in the field of preventing money laundering and terrorist financing by exchanging all information that can facilitate the supervision of obliged persons provided that these third countries have established standards for the prevention of ML and FT, which are equivalent to the provisions of the APMLFT, international standards, or other regulations. Art. 158 states that the BoS, SMA and ISA shall provide European supervisory bodies with all information that is required to enable the performance of their tasks related to preventing money laundering and terrorist financing. Furthermore, the BA in its Art. 16, 19 and 22 regulates the disclosure of information to third parties by the BoS. Art. 22 provides basic modus for cooperation with the competent authorities of the EU Member States and third countries.

435. *Criterion 40.14* - Supervisory authorities can exchange all types of information which is necessary for effective supervision:

a) BoS in line with the BA; SMA in line with the bilateral agreements of cooperation signed;

b) BoS in line with the BA; SMA in line with IOSCO MoU and bilateral MoUs;

c) BoS in line with the BA; SMA in line with IOSCO MoU and bilateral MoUs;

Although the scope of data which should be exchanged for the purpose of the AML/CFT supervision is not specified in the APMLFT, its Art. 156 clearly states that supervisory authorities shall cooperate with competent supervisory bodies from other Member States, particularly by exchanging all

information that could help facilitate the supervision of obliged persons. The same applies for exchanging information with third countries as stipulated in Art. 157 (2) APMLFT.

436. *Criterion 40.15* - Please refer to the text under c.40.8. No information has been provided in relation to the FARS which shall monitor compliance with Art. 67 APMLFT.

437. *Criterion 40.16)* - Under the BA, BoS may further disseminate the information obtained by a supervisory authority from an EU Member State; in such cases, the prior authorisation of the authority is required (Art. 16 (6)). The requirements for cooperation with third countries are established under the respective MoUs.

438. The SMA follows the requirements of c.40.16 in, line with Articles 488 and 488 (a) FIMA. The ISA is authorised to disseminate information exchanged only with the prior authorisation of the requested financial supervisor. Art. 290 IA provides controls and safeguards to ensure that information is used appropriately. The ISA has concluded a number of MoUs with third countries, which, inter alia, also govern the issue of exchange and dissemination of information. No data has been provided with respect to the OMLP.

439. *Criterion 40.17* - Police are permitted to exchange information related to ML, associated predicate offences or FT with foreign counterparts for both - intelligence and investigative purposes. This includes the identification and tracing of the proceeds and instrumentalities of crime. Cooperation with the EU and non-EU Member States is specifically regulated by Art. 11 and 117 of the Police Tasks and Powers Act, as well as by Art. 18, 20 and 38 of the Organisation and Work of the Police Act.

440. Slovenia has also ratified the Convention implementing the Schengen Agreement of 14 July 1985. Police cooperation is defined in Chapter 1 of the said Convention. Art. 39 binds the Contracting Parties to ensure that their police authorities shall, in compliance with national law and within the scope of their powers, assist each other for the purposes of preventing and detecting criminal offences.

441. *Criterion 40.18* - Police can use their powers to conduct inquiries (including investigative powers) and obtain information on behalf of their foreign counterparts as outlined under c.40.8 above. If the request for implementation of investigation activities exceeds police authorisations, the requesting state shall be advised to invite the judicial authorities through MLA. Such authorisation is in line with the provisions of Art. 514 and 515 CPC, and in reference to the Convention on MLA in criminal cases among the EU Member States (Official Gazette MP no. 7/05) and the Protocol to the Convention (Official Gazette - MP no. 7/05). With regard to the exchange of information between police forces, there are numerous bilateral and multilateral agreements and protocols that have been signed between the Slovenian Police and various countries (more details under c.40.3).The information received via Europol and Interpol channels can be used to initiate investigations by the Slovenian police.

442. *Criterion 40.19* - Art. 160a and 160b CPC defines the formation of specialised (SITs) and joint investigative teams (JITs). JITs may include officers of LEAs from another country and may operate in or outside the territory of the Republic of Slovenia. Furthermore, the representatives of competent authorities of the European Union, such as EUROPOL, EUROJUST and OLAF, may also participate in the joint investigation team. The tasks, measures, guidance and other powers must be carried out in accordance with the agreement on the establishment and operation of the JIT. The agreement has to be concluded on the initiative of the State Prosecutor General, the Head of the District State Prosecution Office or the Head of the Specialised Prosecutor's Office of the Republic of Slovenia. It could also be set upon initiative of the competent authority of other state. The State Prosecutor General must notify the MoJ in writing about the concluded agreement. SITs can be established to investigate complex economic and organised crime which usually needs longer and coordinated operations of a number of authorities and institutions. State Prosecutor or his/her representative may, ex officio or upon a written initiative of the police, establish a specialised investigative team together with the heads of individual authorities or institutions. The competent prosecutor is in

charge to manage and direct the work of the team and is also in charge to determine the method of operation of the team.

443. *Criterion 40.20* - Indirect exchange of information between the OMLP and non-counterparts is regulated under Article 113 APMLFT which provides that in order to exchange data, *the provisions of APMLFT contained in the chapter on international cooperation shall apply mutatis mutandis*. Prosecutors are authorised to transmit data from the files, registers, directories and records to the authorities of the EU Member States, third countries and the competent authorities of international organisations if so determined by the law or relevant international treaty. However, personal data can be transmitted only to prosecution authorities or other similar authorities of other state or international organisation. Police can exchange information with LEA of another state only, meaning that there is no operational data exchange with non-counterparts.

444. Slovenian legislation does not specifically ensure that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made.

445. With regard to the supervisory authorities:

- Art. 509 (1) IA allows the ISA to forward confidential information to a large number of non-counterparts. This information can be used by the recipient only for the purpose of exercising their supervisory competencies and tasks and shall remain confidential.

- Similar requirements are set in Art. 488a FIMA allowing the SMA to forward confidential information to a large number of non-counterparts following the conditions described above.

Weighting and Conclusion

446. All of the criteria are under Recommendation 40 are either met or largely met. As concerns criterion 40.2, the law only regulates ISA's cooperation with counterparts from other EU Member States. Concerning Criterion 40.4, the police and ISA do not have a standard procedure for giving feedback to foreign authorities. As concerns criterion 40.7, The Law on Duties and Powers of Police does not expressly provide for the protection of data received from foreign LEAs in the context of international cooperation. No information is available as to the extent to which the OMLP satisfies Criterion 40.16. Concerning criterion 40.20, Police and Prosecution authorities can exchange information only with their counterparts; and Slovenian legislation does not specifically ensure that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made. **Slovenia is rated LC with R.40.**

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
1. Assessing risks & applying a risk-based approach	PC	• The Slovenian NRAs did not include a comprehensive assessment of FT risks and did not explore certain relevant factors in order to properly understand the ML/FT risks. • With the exception of the banking and securities sector, no outreach activities were conducted to inform the private sector of the results of the NRAs. • The Action Plan appears to be rather general, does not include CFT measures and some of its prescribed mitigation activities can be interpreted ambiguously. • Slovenia does not yet apply a risk-based approach to allocate resources and implement measures to prevent or mitigate ML/FT based on understanding of risks. • Exemptions from the application of the FATF Standards and the application of simplified and enhanced CDD requirements are not based on the results of the NRA. • There is no requirement for approval of internal control mechanisms of obliged entities by senior management
2. National cooperation and coordination	LC	• The AML/CFT Action Plan serves as the country's AML/CFT policy and is informed by the findings of the NRA. The NRA, however, does not include a comprehensive assessment of FT risks. • Although a Permanent Coordination Group for Restrictive Measures has been set-up by the Slovenian authorities, the Act which establishes it does not refer specifically to proliferation of weapons of mass destruction.
3. Money laundering offence	LC	• Slovenian legislation does not criminalise the act of ML in the form of simple possession and use of property. • All designated categories of offences with the exception of one are fully covered due to gaps in the FT offence. • There are some minor deficiencies in relation to the scope of application of certain ancillary offences.
4. Confiscation and provisional measures	LC	• The confiscation of instrumentalities from third parties is subject to specific conditions. • The deficiencies in the FT offence (see R.5) limit the possibilities for confiscation of property provided or collected for in FT cases. • Asset tracing measures and provisional measures for instrumentalities are not explicitly regulated in the CPC. • Slovenia does not have a comprehensive system in place for the effective management over time of complex assets, such as active corporate ones.
5. Terrorist financing offence	PC	• The terrorist activities of Art. 108 CC to which the FT offence applies do not include all of the elements of the offences in the treaties listed in the Annex to the FT Convention. • The offences under Art. 108 CC carry an additional purposive terrorist element which is not in line with Art. 2(1)(a) FT Convention. • The FT offence does not cover the financing of a terrorist group or an individual terrorist for a purpose other than the committing of terrorist offences. • The FT offence does not cover all instances of travel for terrorist purposes.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
6. Targeted financial sanctions related to terrorism & FT	PC	• There are no detailed, explicit procedures at the national level in relation to proposing designations to UNSC Committees. • Targeted financial sanctions under UNSCRs 1267/1988 and 1989 are not applied without delay. • The relevant guidelines only address FIs and not DNFBPs (or all natural and legal persons in the country). • There are no national procedures for unfreezing requests. • National procedures for delisting requests are not publicly known.
7. Targeted financial sanctions related to proliferation	PC	• Targeted financial sanctions of UNSCRs relating to the prevention, suppression and disruption of proliferation of mass destruction and its financing are not applied without delay. • The guidelines do not explicitly cover sanctions against proliferation financing. • There are no national procedures for unfreezing requests.
8. Non-profit organisations	PC	• No comprehensive identification has been undertaken to identify the features and types of NPOs which are likely to be at risk of FT abuse or the nature of threats posed by terrorist entities to the NPOs which are at risk as well as how terrorist actors abuse those NPOs. • Founding acts of associations and foundations and annual reports of institutes and foundations are not published online. • No specific outreach to the NPO sector or the donor community on FT issues has been conducted, nor have best practices been developed in cooperation with NPOs to protect them from FT abuse. • Slovenia has not taken steps to promote effective supervision or monitoring over NPOs that demonstrate that risk based measures apply to NPOs at risk of FT abuse. • There is no obligation on foundations to keep or register updated information on members of the Board of Trustees. • There are no requirements on NPOs to take reasonable measures to confirm the identity, credentials and good standing of beneficiaries and associate NPOs and to confirm that they are not involved with or financially support terrorists or terrorist organisations. • Except for associations, there are no bodies with powers to conduct inspections of NPOs' activities. • Administrative sanctions on NPOs for failure to communicate changes to authorities are not sufficiently dissuasive. • There are no mechanisms for regular information-sharing between the various competent authorities involved in registration and supervision of NPOs in order to identify and monitor NPOs at risk.
9. Financial institution secrecy laws	LC	• Absence of explicit exemptions from confidentiality provisions related to the exchange of information between FIs
10. Customer due diligence	LC	• With regards to wire transfers above EUR 1,000, the requirement does not include the full range of CDD measures such (e.g. identifying and verifying the beneficial owner). • There are some gaps in the definitions of beneficial owner for legal persons and in requirements regarding how the beneficial owner of a natural person shall be ascertained.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		• Absence of legal requirement for FIs to take reasonable measures to verify the identity of beneficial owner, using relevant information or data obtained from reliable source. • There are no requirements for FIs to include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable. • the scope of the delay of completing the verification of customer and beneficial owner is wider that that permitted under criterion 10.14. • FIs are not required to adopt risk management procedures under which the customer can utilise the business relationship prior to verification. • There is no explicit requirement to conduct CDD for existing customers. • There is no provision in the law that allows FIs not to pursue CDD requirements where they suspect ML or FT and reasonably believe that performing the CDD process will tip off the customer.
11. Record keeping	C	
12. Politically exposed persons	PC	• Absence of requirement to take reasonable measures to ascertain the sources of wealth and funds of the beneficial owner identified as a PEP. • Unclear whether requirement to obtain a senior management approval applies also to beneficial owner that becomes a PEP.
13. Correspondent banking	PC	• Application of additional measures by FIs is limited only to cross-border correspondent relationships with credit institutions from non-EU member countries. • No explicit requirement for FIs to understand the nature of the respondent's business. • No requirements for FIs to understand the responsibilities of each institution, and to conduct the assessment of a respondent institution's AML/CFT controls. • The additional measures provided by APMLFT are insufficient to require FIs to determine the reputation of a respondent or the quality of supervision applied to it. • There are no specific requirements provided for by the AML/CFT legislation with respect to payable-through accounts. • Absence of explicit requirement for FI to be subject to an "effective" supervision in order to not be considered as a shell bank as required by the FATF standards.
14. Money or value transfer services	C	
15. New technologies	C	
16. Wire transfers	PC	• The EU regulation in force does not cover beneficiary information and contains limited requirements for intermediate financial institutions, which affects almost all the criteria in this Recommendation
17. Reliance on third parties	LC	• Lack of requirement for FIs to satisfy themselves that third parties established in EU Member States are regulated, and supervised or monitored for, and have measures in place for compliance with appropriate CDD and record-keeping

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		obligations. • Permitting reliance on EU-based FIs or their branches and majority-owned subsidiaries in third countries as third parties on the basis of the presumption that all EU-based FIs would ensure application of appropriate AML/CFT measures is the deficiency. • No specific requirement to adequately mitigate the higher country risk at the group level.
18. Internal controls and foreign branches and subsidiaries	LC	• It is not specified that policies, controls and procedures should cover also training. • Further explanation as to the implementation of group policies and procedures needs to be defined in sector specific guidance. • The law requires the implementation of policies and procedures of a group and measures for detecting and preventing ML/FT in branches and majority-owned subsidiaries located in third countries, however there is no provision for branches and subsidiaries in EU countries as the term "third countries" within the APMLFT does not include the EU member states. • Obliged entities have obligation to ensure that the measures for detecting and preventing ML/FT are also implemented at equal or higher level in its branches and its majority-owned subsidiaries established in 'third countries' which does not include the EU member states. • Provisions regulating the sharing of information by the obliged person with its group do not include sharing of information by branches and subsidiaries, outside Member States, with the obliged person.
19. Higher-risk countries	LC	• There is no explicit requirement in the law or other enforceable means to apply enhanced due diligence proportionate to the risks to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF. • The limitation of the "special care" provision only to unusual transactions does not enable the provision of a wide range of countermeasures that can be applied proportionately to risks.
20. Reporting of suspicious transaction	C	
21. Tipping-off and confidentiality	C	
22. DNFBPs: Customer due diligence	LC	• Deficiencies in the legal and regulatory framework related to CDD requirements, PEPs and "reliance of third parties" affect the compliance on these matters.
23. DNFBPs: Other measures	LC	• Deficiencies identified under Recommendations 18, 19 and 21 are also applicable to compliance with Recommendation 23.
24. Transparency and beneficial ownership of legal persons	LC	• Slovenia did not assess the ML/FT risks associated with all types of legal persons created in the country. • The instructions on determination of beneficial ownership in the APMLFT may lead to some potential beneficial owners of legal persons to be missed. • The current mechanism to obtain beneficial ownership information on legal persons (through obliged entities

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
		performing CDD measures) does not ensure that information is as up-to-date as possible for all legal persons in the country. • Authorised representatives of legal persons, who can be held accountable to cooperate with authorities to determine the beneficial owner, are not required to be resident in the country. • Slovenia does not apply sufficient mechanisms to ensure that nominee shares and nominee directors are not misused. • The quality of assistance received from other countries in response to requests for beneficial ownership information is not monitored.
25. Transparency and beneficial ownership of legal arrangements	LC	• No all-encompassing obligation on trustees or managers of mutual funds acting on behalf of investors to disclose their status to FIs and DNFBPs. • The current mechanism to obtain beneficial ownership information on legal arrangements (through CDD measures by obliged entities) does not ensure that information is as up-to-date as possible for all legal arrangements in the country.
26. Regulation and supervision of financial institutions	PC	• Fit and proper requirements do not apply to beneficial owners in all situations. • There is no explicit requirement for supervisors to review periodically the assessment of the ML/FT risk profile of a FI or group (including the risk of non-compliance).
27. Powers of supervisors	C	
28. Regulation and supervision of DNFBPs	PC	• The basic infrastructure for sound regulation and supervision of DNFBPs has gaps (c.28.1, c.28.3) • There is also weakness in the implementation of a risk based supervisory approach (c.28.5).
29. Financial intelligence units	C	
30. Responsibilities of law enforcement and investigative authorities	C	
31. Powers of law enforcement and investigative authorities	LC	• The provisions regulating controlled delivery are not sufficiently wide in scope.
32. Cash couriers	PC	• The declaration system applies only to movements (both inward and outward) of cash and BNI from and to the EU - movements of cash and BNI within the EU are not considered to be cross-border movements under the Foreign Exchange Act. • The legislation does not explicitly provide the Customs administration with the abilities to freeze or restrain currency or BNIs for a reasonable time in order to ascertain whether evidence of ML/FT exist.
33. Statistics	LC	• The legislation does not explicitly impose the relevant authority - Ministry of Justice any obligation to keep statistics on MLA.
34. Guidance and feedback	C	
35. Sanctions	C	
36. International instruments	LC	• Shortcomings under R.3, 4, 5, 31 and 32 impact on compliance with R.36. • The asset recovery requirements of Art. 14(2) Palermo Convention, Art. 8(4) FT Convention, and Art. 51 and 53 Merida Convention do not appear to be implemented.

Compliance with FATF Recommendations		
Recommendation	**Rating**	**Factor(s) underlying the rating**
37. Mutual legal assistance	LC	• Deficiencies observed in relation to R. 3 and 5 may restrict the range of mutual assistance in cases where dual criminality is required.
38. Mutual legal assistance: freezing and confiscation	LC	• Deficiencies observed in relation to R. 3 and 5 may restrict the range of mutual assistance in cases where dual criminality is required in the case of a freezing or confiscation request relating to certain ML/FT offences. • Deficiencies observed under R. 4 (in relation to tracing and provisional measures of instrumentalities, and with regard to mechanisms for asset management) cascade on R. 38.
39. Extradition	LC	• Certain deficiencies relating to the ML/FT offences may limit the scope of extradition measures.
40. Other forms of international cooperation	LC	• The law does not regulate ISA's cooperation with non-EU Member State counterparts. • It cannot be concluded that all competent authorities provide feedback in a timely manner to competent authorities from which they have received assistance. • The protection of data received from foreign LEAs in the context of international cooperation is not expressly provided by the law. • No information is available as to the extent to which the OMLP satisfies Criterion 40.16. • Police and Prosecution authorities can exchange information only with their counterparts; • Slovenian legislation does not specifically ensure that the competent authority that requests information indirectly always makes it clear for what purpose and on whose behalf the request is made

© MONEYVAL

www.coe.int/MONEYVAL

June 2017

Anti-money laundering and counter-terrorist financing measures

Slovenia

Fifth Round Mutual Evaluation Report

This report provides a summary of the AML/CFT measures in place in Slovenia as at the date of the on-site visit (7-18 November 2016). It analyses the level of compliance with the FATF 40 Recommendations and the level of effectiveness of Slovenia's AML/CFT system, and provides recommendations on how the system could be strengthened.