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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MONEYVAL(2026)7

Anti-money laundering and counter-terrorist financing measures

Slovenia

Sixth Round Mutual Evaluation Report

May 2026

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

The sixth round mutual evaluation report on Slovenia was adopted by the MONEYVAL Committee at its 71st Plenary Session (Strasbourg, 27-29 May 2026).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report summarises the AML/CFT measures in place in Slovenia as at the date of the on-site visit (10.10.2025). 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.

Key Findings

a) Slovenia's understanding of ML/TF risks is informed by two successive NRAs completed in 2021 and 2025. The country's understanding of ML risks is largely adequate and more sophisticated than that of TF, with prosecutors, law enforcement agencies (LEA) and financial sector supervisors, primarily the Bank of Slovenia (BoS), having more developed understanding of ML/TF risks than non-financial supervisors in the DNFBP sectors. Although NRA action plans contribute to guiding national AML/CFT actions to some extent, Slovenia lacks a formal national AML/CFT strategy with an integrated, prioritised, and adequately resourced framework to ensure that policy actions, effectively address and mitigate the country's key ML/TF risks. The BoS activities are aligned with the risks identified in the NRAs, but other supervisors and SRBs, particularly in the DNFBP sectors, have not embedded NRA findings into their activities. LEAs and judicial authorities are reactive to criminality rather than proactively aligning their activities with the identified ML/TF risks. While policy-level coordination remains less developed, operational coordination mechanisms exist between LEAs, prosecutors and the OMLP. Informal operational cooperation between the OMLP, financial supervisors and reporting entities is effective, but structured inter-agency information-sharing and typology exchanges are limited.

b) Slovenia provides constructive, timely and effective cooperation to foreign counterparts employing alternative measures when necessary to ensure the objectives of foreign requests are met. The legal assistance is mostly focused on EU member states, but the authorities demonstrate that they effectively cooperate outside of the EU borders. The authorities' efforts are broadly in line with country's risk profile. Nevertheless, there is a lack of comprehensive statistics on cooperation with EU Member States that limits Slovenia's capacity to fully the monitor the effectiveness of this cooperation. Slovenian authorities have actively participated in joint investigation teams (JITs), both as initiators and partners, with their swift cooperation being particularly valued. Yet, the asset tracing efforts are not entirely proactive. Other forms of international cooperation are also broadly used to facilitate criminal investigations and asset recovery and to support supervisory actions related to ML and TF.

c) Slovenia has shown and has overall good effectiveness in market entry controls for FIs and has recently aligned requirements for the VASP sector. Authorities are more proactive in detecting unauthorised activities than in ongoing fit and proper monitoring. While sector-specific risk assessments have not been conducted, authorities demonstrate risk awareness through the NRA process. AML/CFT supervisors have risk assessment procedures for OEs, though depth varies by sectors. FIs and VASPs show strong awareness of sector risks and

AML/CFT/CPF obligations. Supervisory examinations occur to varying extents, full-scope exams being low in number but generally reflecting sector risk levels. A range of remediation and enforcement actions are applied. However, reliance on misdemeanour procedures to impose fines at times reduces penalty amounts and affects the proportionality and timeliness of sanctions.

d) Licensing and registration frameworks exist for DNFBPs in Slovenia but there are fundamental weaknesses. Market entry controls are absent for preventing criminal associates from owning or managing OEs, and detection of unauthorised operators is also weak. There are no market entry controls for tax advisors, accountants, or DPMS, and it is unclear if legal advisors (not registered with SBA) perform activities that fall under FATF Standards despite identified higher ML risk. Supervisors' understanding of ML/TF risks (except for FARS) is largely limited to the NRA findings with no comprehensive or effective independent risk assessment conducted either at sectoral or individual entity level. DNFBPs, except for casinos and internationally active accountants and auditors, showed an overall limited understanding of ML/TF risks and their obligations, even in higher-risk sectors. Supervisory authorities and SRBs have limited staff and budgets, resulting in weak supervision that is primarily resource-driven rather than risk-based. Remedial and enforcement actions are weak, inconsistent, and lack deterrent effect.

e) Slovenia's NRA provides some insights into how legal persons (LP) can be abused for ML/TF with authorities demonstrating varying levels of understanding of risks. All LPs have to be registered in Slovenia. Basic information is publicly accessible through the Slovenia's Business Register (SBR). The adequacy of BO information is ensured through Slovenia's system of publicly accessible registers, which also includes the Register of Beneficial Ownership (RBO). Authorities undertook a series of actions to ensure that the RBO is fully populated. Over 95% of LPs hold bank accounts in Slovenia. FIs, especially banks, have a more in-depth knowledge of the concept of BO compared to other OEs from less material sectors. The supervisory activity by AML/CFT supervisors does not ensure that BO information held by all OEs, especially within the DNFBP sector, is accurate and updated in a timely manner. Consequently, the BO information available in the RBO may not be fully accurate and up-to-date. Sanctions against LPs do not seem to be proportionate, effective and dissuasive.

f) The OMLP has extensive and timely access to a broad range of databases enabling it to perform its functions. While LEAs have also direct and indirect access to various databases, recent legislative amendments have limited their access to banking information of natural persons, which to some degree hinders their effective performance. The OMLP produces and disseminates operational analysis which is used to support needs of other competent authorities to some extent. The insufficient resources and the shortcomings in its manual prioritisation mechanism for STRs have limited the OMLP's ability to produce financial intelligence in a timely manner, particularly with respect to ML cases. The OMLP effectively prioritises TF-related STRs and ensures timely dissemination to the police. While strategic analysis is produced to some extent, the absence of the relevant methodology and dedicated fulltime staff coupled with the gap in STRs from DNFBPs and FIs besides banks hinders the OMLP's ability to detect and follow evolving ML/TF trends and typologies. The OMLP closely and effectively cooperates with other competent authorities and exchanges information, although issues are observed with respect to confidentiality and security of the disseminations done via the post.

g) LEAs identify and investigate a number of ML cases and systematically conduct parallel financial investigations alongside investigations of predicate offences. A range of investigative powers are available to investigators, yet recent CPA amendments limit their use during the pre-investigation stage of ML and associated predicate offences. While authorities can pursue all types of ML offences, the high evidentiary threshold established by jurisprudence hampers the effective identification and investigation of autonomous ML offences. The majority of ML cases stem from fraud, with some linked to property from drug trafficking, reflecting the country's risk profile to some extent. Undue delays in criminal proceedings have an impact on sanctions being lenient.

h) The competent authorities (police and prosecutors) prioritise asset recovery through their own policies; however, their efforts are hampered by insufficient ministerial support and inadequate resources. While cooperation and information exchange in asset recovery between competent authorities are effective, the absence of comprehensive central records and data undermines the overall effectiveness of the confiscation regime. Asset tracing and recovery remain mandatory elements of all investigations into acquisitive crime which has resulted in a commendable value of criminal property being seized. Victims are able to seek recovery of funds within criminal proceedings, with victim compensation taking priority over confiscation. Despite indications of significant volumes of cash entering or transiting the jurisdiction, the identification and seizure of undeclared or falsely declared cash remain limited.

i) Slovenia has a sound legal and institutional framework for combating TF. A variety of sources is used to identify TF activity, yet proactive identification of potential TF activity is rare. The competent authorities (FIU, Police and SOVA) demonstrate strong operational cooperation among its competent authorities leading to the identification and pre-investigation of 16 TF cases which is in line with country's TF risk profile. Slovenia has not prosecuted any TF cases and has not had any TF convictions. Nevertheless, there are measures in place indicating that Slovenia is prepared to deal with TF prosecutions and judicial proceedings once they occur. Slovenia has developed a National Strategy on Prevention of Violent Extremism and Terrorism with some TF elements. However, it was not informed by intelligence obtained through TF investigations.

j) TF and proliferation financing (PF) targeted financial sanctions (TFS) are implemented in Slovenia without delay, but major issues remain with communication of designations and the reporting of frozen assets. Slovenia has a procedure and a mechanism for identifying targets for designation, however, no designations were made or proposed by Slovenia under the UNSCRs, which is in line with its TF risk profile. Slovenia conducted its first PF risk assessment within the 2025 NRA. Its comprehensiveness is limited. Nevertheless, the overall risk and context of the country entail no major risk of PF. Material FIs and VASPs have a solid understanding of their TFS obligations and established effective policies, procedures and controls to ensure compliance with them, and those are regularly supervised, which is not a case with DNFBPs.

Effectiveness & Technical Compliance Ratings

	Effectiveness		Technical Compliance	
Risk mitigation through policy, co-ordination and co-operation				
Assessment of risk, coordination and policy setting	**IO.1**	ME	**R.1**	PC
			R.2	PC
International co-operation	**IO.2**	SE	**R.36**	LC
			R.37	LC
			R.38	LC
			R.39	LC
			R.40	LC
Cross-cutting requirements			**R.33**	LC
Prevention, detection & reporting of illicit funds across sectors				
Financial sector and virtual asset supervision and preventive measures	**IO.3**	SE	**R.9**	LC
			R.10	LC
			R.11	C
			R.12	C
			R.13	LC
			R.14	C
			R.15	PC
			R.16	LC
			R.17	LC
			R.18	LC
			R.19	LC
			R.20	LC
			R.21	LC
			R.26	LC
			R.27	LC
Non-financial sector supervision and preventive measures	**IO.4**	LE	**R.22**	PC
			R.23	LC
			R.28	PC
Transparency and beneficial ownership	**IO.5**	ME	**R.24**	PC
			R.25	PC
Cross-cutting requirements			**R.34**	LC
			R.35	PC
Detection and disruption of threats, sanctions & deprivation of illicit funds				
Financial intelligence	**IO.6**	ME	**R.29**	C
Money laundering investigations and prosecutions	**IO.7**	ME	**R.3**	LC
Asset recovery	**IO.8**	ME	**R.4**	PC
			R.32	LC
Terrorist financing investigations and prosecutions	**IO.9**	ME	**R.5**	LC
Terrorist financing preventive measures and financial sanctions	**IO.10**	ME	**R.6**	LC
			R.8	PC
Proliferation financing financial sanctions	**IO.11**	ME	**R.7**	LC
Cross-cutting requirements			**R.30**	C
			R.31	LC

Note: Effectiveness ratings can be either a High- HE, Substantial- SE, Moderate- ME, or Low – LE, level of effectiveness. Technical compliance ratings can be either a C – compliant, LC – largely compliant, PC – partially compliant or NC – non-compliant. While the technical compliance findings can be relevant across the effectiveness immediate outcomes (for example, R.1 or R.40), the table above illustrates the main technical compliance findings specific to each effectiveness immediate outcome and cross-cutting requirements for each of the intermediate outcomes. For more detail on the relevant technical compliance requirements relevant to each effectiveness immediate outcome, see the relevant paragraph at the beginning of each chapter. See also paragraphs 53 and 54 of the FATF 2022 Methodology for links between effectiveness and technical compliance ratings.

Risks and General Situation

1. Since 2017 MER, Slovenia's risk profile has remained largely stable. While not being a financial centre, Slovenia's financial sector is dominated by banks, with significant importance also attached to electronic money institutions and VASPs, other financial sectors and DNFBPs having significantly smaller market share. Main ML threats stem from proceeds of economic crime (abuse of office, tax evasion, business fraud) and organised crime (trafficking in drugs, weapons, people, and smuggling), classic property crime (mainly relating to online fraud and attacks on information systems), and corruption. Given Slovenia's geographical position as a transit country between the Balkans and Western Europe, the country is also exposed to external threats arising from cross-border crime, including cross-border laundering through cash, and the activities of foreign nationals. TF risk is assessed as low.

2. Since the last evaluation, Slovenia has made efforts to strengthen its AML/CFT system. It has demonstrated substantial or moderate level of effectiveness with all Immediate Outcomes (IO), with the exception of IO.4 which has been assessed as low. With respect to technical compliance, the country has also made progress, further aligning its legislation and institutional framework with FATF standards, with the majority of recommendations having been assessed as largely compliant or compliant except for R.1, R.2, R.4, R.8, R.15, R.22, R.24, R.25, R.28, R.35 which are assessed as partially compliant.

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

3. Slovenia has made considerable efforts to improve its understanding of ML/TF risks through two successive NRAs completed in 2021 and 2025. Particularly the 2025 NRA shows improved methodological standards, increased variety of datasets analysed, expanded coverage of sectors, a more comprehensive assessment of cross-border ML, and greater inclusion of emerging typologies such as cyber-enabled fraud and virtual assets. However, while the overall threat landscape is broadly identified, the robustness of Slovenia's ML/TF risk assessment remains constrained by structural data limitations and uneven sectoral engagement.

4. Prosecutors, LEAs and the BoS demonstrated stronger understanding of ML/TF risks in comparison with other financial and non-financial supervisors. The BoS activities are aligned with the risks identified in the NRAs, but other supervisors and SRBs, particularly in the DNFBP sectors, have not embedded NRA findings into their activities. While having adequate understanding of risks, LEAs and judicial authorities are reactive to criminality rather than proactively aligning their activities with the identified ML/TF risks.

5. In the absence of the national AML/CFT strategy, the country lacks an integrated, prioritised, and adequately resourced framework to ensure that policy actions, effectively address and mitigate the country's ML/TF risks. While policy-level coordination remains significantly weaker and less developed, operational coordination mechanisms exist between LEAs, prosecutors and the OMLP. Informal operational cooperation between the OMLP, financial supervisors and reporting entities is effective, but structured inter-agency information-sharing and typology exchanges are limited.

International co-operation (Chapter 2; IO.2; R.36–40)

6. Slovenia provides constructive, timely, and effective international cooperation in criminal matters, grounded in international instruments and the principle of reciprocity. While most legal

assistance focuses on EU member states, Slovenian authorities have shown they can effectively cooperate beyond EU borders.

7. Slovenian authorities efficiently execute requests for assistance and extradition, using alternative measures when certain actions are not available under domestic law to ensure that the objectives of foreign requests are met. The authorities do seek assets moved abroad and are effective when executing foreign request for freezing, seizing and confiscation. Nevertheless, their efforts in tracing assets moved abroad cannot be considered as fully proactive. Comprehensive statistics on cooperation with EU partners are lacking, which limits the country's ability to develop a full overview of crime trends and to fully monitor effectiveness of this cooperation.

8. Active participation in joint investigation teams (JITs), whether initiated by Slovenia or its international partners, underscores the country's commitment to collaborative efforts, with the efficiency of this cooperation being particularly noted. Furthermore, Slovenian authorities make extensive use of informal cooperation channels to facilitate criminal investigations, support asset recovery, and enhance supervisory actions related to ML and TF.

Financial sector and virtual asset supervision and preventive measures (Chapter 3; IO.3, R.9-21, 26, 27, 34 & 35)

9. The authorities demonstrate overall good effectiveness in restricting criminals and their associates from entering the ownership and control of FIs. Regulatory requirements for virtual asset service providers (VASPs) have been aligned with those for material FIs. Authorities adopt a more proactive approach to identifying unauthorised activities, though a reactive stance generally prevails regarding ongoing fit and proper assessments.

10. While sector-specific risk assessments are not undertaken, active participation in the NRA enables authorities to maintain effective risk awareness over FIs and VASPs under their remit. All main AML/CFT supervisors demonstrated to have risk assessment processes OEs, though the scope and depth vary between sectors.

11. FIs and VASPs concur with the NRA findings, particularly key institutions, which can articulate their primary ML/TF risks and mitigation strategies. Authorities provide guidance and training, enhancing the ability of OEs to meet AML/CFT obligations. This may account for the good grasp of their obligations that the OEs have shown.

12. Supervisory examinations occur to varying extents, full-scope exams being low in number but generally reflecting sector risk levels. A wide range of supervisory measures, including follow-up actions and pecuniary fines, are applied to address deficiencies. Where timely remediation is lacking, further enforcement measures are pursued. The use of misdemeanour procedures to impose fines restricts sanctioning effectiveness and proportionality.

Non-financial sector supervision and preventive measures (Chapter 4; IO.4, R.22, 23, 28, 34 & 35)

13. Licensing and registration frameworks exist for DNFBPs in Slovenia, but are undermined by an administrative approach, reliance on self-certification, and significant regulatory gaps. Market entry controls do not prevent criminal associates from ownership or management, and detection of unauthorised entities is weak. There are no market entry controls for tax advisors, accountants, or DPMS, and there is no clarity whether legal advisors (not registered with SBA) perform activities that fall under FATF Standards even though the 2025 NRA identifies the group as posing a higher ML risk.

14. Supervisors' understanding of ML/TF risks and implementation of AML/CFT obligations is generally weak, with limited integration of NRA findings into supervisory frameworks. Risk assessments at sectoral and entity level remain incomplete and ineffective, with the FARS being the only supervisor demonstrating a more developed understanding. DNFBPs similarly show limited understanding of their risks and were unable to articulate the practical application of their AML/CFT obligations, with the exception of casinos and internationally active accountants and auditors, which benefit from stronger controls and group-level frameworks. While training and guidance is provided to DNFBPs, these measures remain insufficient to address ongoing deficiencies in understanding and awareness of ML/TF risks and AML/CFT obligations.

15. Supervisory authorities and SRBs face significant resource constraints, resulting in weak and predominantly resource-driven supervision. Effective supervision is further impeded by the lack of, or incomplete, data on OEs and their activities. The use of sanctions is infrequent, with enforcement primarily consisting of warnings and remedial measures. Overall, sanctions are modest, inconsistent, and lack a sufficiently dissuasive effect.

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

16. In the 2025 NRA, Slovenia has taken some steps to understand and assess the ML/TF risks presented by domestic and foreign LPs. This understanding is impacted by insufficient analysis of data related to the presence of the strawmen, shelf and shell companies and LLCs subjected to investigations by LEAs being liquidated on an annual basis. Although some authorities have a deeper understanding of how LPs can be abused in specific areas, there is the need to form a commonly shared understanding of ML/TF risks. Being a less pressing issue due to the inability to establish trusts and similar arrangements under Slovenian law together with its limited exposure to this phenomenon, the possible ML/TF risks associated with legal arrangements have not been considered in the 2025 NRA.

17. Slovenia has also taken some steps to prevent the abuse and to increase the transparency of LPs and legal arrangements. Slovenia established multiple interconnected national registers, with the SBR and the RBO holding significant basic and BO information, albeit the RBO is not yet fully populated. Additional safeguards include a degree of checks carried out on the founders of most LPs and the prohibition of nominee directors and shareholders. Over 95% of LPs hold bank accounts in Slovenia. FIs, especially banks, have a more in-depth knowledge of the concept of BO compared to other OEs from less material sectors. This notwithstanding, there are some shortcomings to ensure that the basic and BO information accessible by the authorities is accurate and current. The supervisory activity by AML/CFT supervisors does not ensure that BO information held by all OEs, especially within the DNFBP sector, is accurate and updated in a timely manner.

18. Sanctions against LPs do not seem to be proportionate, effective and dissuasive, with only a low number of warnings and/or fines having been imposed as primary focus has been placed on remediation.

Financial intelligence (Chapter 6 ; IO.6, R.29 - 32)

19. The OMLP has extensive and timely access to a broad range of databases enabling it to perform its functions. While LEAs have also direct and indirect access to various databases, recent legislative amendments have limited their access to banking information of natural persons, which to some degree hinders their effective performance. The insufficient resources and the shortcomings

in its manual prioritisation mechanism for STRs limit the OMLP's ability to produce financial intelligence in a timely manner, particularly with respect to ML cases. The OMLP effectively prioritises TF-related STRs and ensures timely dissemination to the police. OMLP's analytical products are used to support the needs of LEAs and other competent authorities to some extent. While certain strategic analysis is produced, the absence of the relevant methodology and dedicated fulltime staff coupled with the gap in STRs from DNFBPs and FIs besides banks hinders the OMLP's ability to detect and follow evolving ML/TF trends and typologies.

20. The OMLP has good and regular cooperation with other competent authorities, particularly with the Police, including through special investigative teams. The authorities consider cooperation to be very effective, but its results are not confirmed by the low number of criminal investigations initiated for ML/TF. Issues observed in relation to confidentiality and security of the process for dissemination of financial intelligence by the OMLP, which is done in hard copies, raise concerns, especially with respect to disseminations sent via the post to local police units.

Money laundering investigations and prosecutions (Chapter 7; IO.7, R. 3, 30 & 31)

21. Slovenia has established legal and institutional frameworks to identify and investigate ML offences, with dedicated teams within LEAs and the prosecutor's office entrusted to handling complex cases. ML investigations are initiated from various sources, including parallel financial investigations. A variety of investigative powers are available to the investigators, however, recent legislative amendments raised evidential thresholds for authorising special investigative measures, hindering the identification and investigation of ML offences.

22. Prosecutors predominantly focus on self-laundering and third-party ML linked directly to established predicate offences, reflecting judicial interpretations that require a confirmed predicate offence before pursuing ML cases. While authorities acknowledge that this approach discourages the investigation and prosecution of autonomous ML, measures to address this limitation are being considered, though tangible results remain limited.

23. Most ML cases originate from fraud, with some involving property derived from drug trafficking, partially reflecting Slovenia's risk profile. Nevertheless, a clear disparity exists between the number of predicate offences and the comparatively low number of ML investigations.

24. Sanctions for ML are presently not seen as effective, proportionate, or dissuasive, and undue delays in criminal proceedings often result in reduced penalties, further weakening their impact.

25. In cases where ML convictions are not feasible, authorities often pursue charges for predicate offences and apply non-conviction based confiscation.

Asset recovery (Chapter 8; IO.8, R. 1, 4 & 32)

26. Slovenian authorities have made asset recovery a priority in their fight against acquisitive crime, integrating asset tracing and recovery into all relevant investigations and demonstrating strong cooperation and information exchange among competent bodies. Provisional measures to freeze and seize criminal property are frequently employed, resulting in the recovery of significant assets. However, these efforts are hampered by limited ministerial support and resourcing, the absence of a comprehensive and centralised data system, and challenges related to higher evidentiary thresholds for obtaining banking information.

27. The management of seized and frozen assets is distributed among several authorities, each maintaining their own records, which has led to fragmentation and deficiencies in effective oversight. While both conviction-based and non-conviction-based confiscation methods are available, the use of non-conviction-based confiscation remains limited. The effectiveness of asset recovery is further undermined by the lack of comprehensive data, inconsistent use of pre-confiscation sales to prevent asset dissipation, and vulnerabilities in victim compensation practices that may allow offenders to benefit through corporate entities.

28. Additionally, the identification and seizure of undeclared or falsely declared cash remains limited despite the significant cash flows observed in and through Slovenia. Sanctions for failures to declare cash are not sufficiently effective, proportionate, or dissuasive.

29. Overall, while operational cooperation is strong and authorities have secured a commendable value of criminal property, further improvements are necessary to enhance the overall effectiveness and integrity of Slovenia's asset recovery regime.

Terrorist financing investigations and prosecutions (Chapter 9; IO.9, R. 5, 30, 31 & 39)

30. Slovenia has established a sound legal and institutional framework for combating TF, with competent authorities demonstrating good cooperation and a solid understanding of the offence. A variety of sources are used to identify TF activity; however, proactive identification remains limited, as tools such as OSINT and strategic analysis are not systematically employed to detect potential TF trends and techniques.

31. Since 2020, authorities have launched multiple pre-investigations into TF, but all have been dismissed, and to date, there have been no prosecutions or convictions for TF-related offences. While the preparation for TF prosecutions appears robust—evidenced by specialised and regularly trained prosecutors and judges—the absence of cases prevents a comprehensive assessment of prosecution effectiveness and the application of sanctions.

32. There is National Strategy on Prevention of Violent Extremism and Terrorism with some TF elements incorporated, yet the strategy was not informed by TF investigations.

Terrorist financing preventive measures and financial sanctions (Chapter 10; IO.10, R. 1, 4, 6 & 8)

33. TF TFS under UNSCRs 1267/1989, 1988, and 1373 are implemented in Slovenia without delay. Slovenia has procedures for designations but has made none, consistent with its TF risk profile. Nevertheless, implementation is hindered by the absence of a proactive mechanism to notify OEs and the public about designations, while FIs and VASPs use commercial screening tools. The TFS guidance has not been properly communicated—except to FIs supervised by the BoS—mainly due to limited resources at the MFEA.

34. Slovenia's TFS governance has major weaknesses: unclear communication channels, absence of a central authority and reporting formats, lack of TFS statistics, and inability to demonstrate actions taken on reported cases.

35. FIs and VASPs understand and largely comply with TF-related TFS obligations. DNFBPs show low awareness and compliance. Supervisors effectively monitor FIs and VASPs, but there are significant deficiencies in monitoring DNFBPs' TF-related TFS compliance.

36. Slovenia assessed TF risks of the NPO sector, but did not properly identify high-risk NPOs or apply risk-based mitigation. Oversight of NPOs is fragmented and uncoordinated, and measures applied are not focused, proportionate and risk-based.

Proliferation financing financial sanctions (Chapter 11; IO.11, R. 7)

37. Slovenia has established a Standing Coordination Group (SCG), bringing together a broad range of authorities to ensure consistent implementation of UN TFS on PF. Effective operational cooperation exists between SOVA, the Police, and OMLP. While Slovenia's Foreign Policy Strategy generally addresses counter-proliferation issues, there is no dedicated policy on combating proliferation financing (CPF).

38. Slovenia's first PF risk assessment, conducted as part of the 2025 NRA, was limited in scope. Overall, PF risk was assessed as low, including the risk of breaches or evasion of PF-related TFS by banks and DNFBPs. However, VASPs were assessed to face a medium-high PF threat. Slovenia has not shown specific measures in place to mitigate these PF risks.

39. Mechanisms set for implementation of TFS of PF under UNSCR 1718(2006) on DPRK and its successor resolutions are similar to those set for the TF-related TFS, sharing similar strengths and weaknesses of the effective implementation of measures, including the performance of the private sector.

Key Recommended Actions (KRA) Roadmap

1. The Republic of Slovenia underwent a Mutual Evaluation of its anti-money laundering / countering the financing of terrorism / countering proliferation financing (AML/CFT/CPF) measures in place during its on-site visit to the country from 29 September – 10 October 2025. This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the 2022 Methodology.

2. The Mutual Evaluation Report identifies the strengths and weaknesses of Slovenia's AML/CFT/CPF system, including both the level of effectiveness and the level of technical compliance, and recommended actions for improvement. The highest priority measures are identified as Key Recommended Actions (KRA) are included in this KRA Roadmap.

3. The following presents the KRA Roadmap for the Republic of Slovenia as adopted by MONEYVAL Plenary in May 2026. Based on Effectiveness and Technical Compliance Ratings, Slovenia is placed in enhanced follow-up. This KRA Roadmap also serves as the basis for Slovenia's follow-up process.

IO.1 (Assessment of risk, coordination and policy setting)

a) Slovenia should enhance its risk-based approach by establishing a formal national AML/CFT strategic framework through the adoption of national policies with (i) strategic priorities and measurable objectives aligned with the findings of the 2025 NRA; (ii) clear division of responsibilities and reasonable timeframes for implementation; (iii) mechanisms for coordination, monitoring, periodic review, and reporting on progress. Furthermore, all competent authorities should establish their own strategies and policies in line with the national framework, ensuring that the findings of the 2025 NRA are systematically embedded into their operational objectives, activities, and enforcement priorities.

b) Slovenia should significantly strengthen its high-level policy coordination in combatting ML and TF by: (i) formalising working group governance arrangements and providing the groups with the relevant policy making authority, and (ii) providing the necessary resources for dedicated staff to be able to manage their required obligations.

IO.2 (International co-operation)

N/A

IO.3 (Financial sector and virtual asset supervision and preventive measures)

N/A

IO.4 (Non-financial sector supervision and preventive measures)

c) Slovenia should conduct a comprehensive assessment of the legal advisors' sector to determine the activities and services provided by those. When those fall within the scope of the FATF Standards, Slovenia should (i) assess the ML/TF risks associated with the sector, and (ii) establish and implement a regulatory and operational supervisory framework, including effective market entry requirements.

d) Slovenia should: (i) set registration or licensing frameworks and appoint a designated competent authority or SRB, for Tax Advisors, Accountants, and all types of DPMSs; (ii) considerably strengthen the market entry framework, including verification of information on criminal background (except for the casino sector), ongoing fitness and properness checks, and introduce checks on criminal association; and (iii) establish clearly documented detection and termination policies and procedures of unauthorised operators (except for the casino sector).

e) Slovenia should increase supervisory capacities, including human resources at MIRS, SRBs and the OMLP, and ensure that ML/TF risks of DNFBPs are comprehensively identified, understood and regularly monitored, and that the risk-based approach is applied in supervision and monitoring.

IO.5 (Transparency and beneficial ownership)

f) Slovenia should assess the ML/TF risks presented by domestic and foreign LPs as well as legal arrangements, using widest range of datasets and information and analysing aspects like strawmen, the phenomenon of struck-off companies and the use of shelf and shell companies. Slovenia should take commensurate measures to address and mitigate any identified risks.

g) To limit the potential misuse of LPs for ML/TF purposes, Slovenia should strengthen the existing mechanisms and introduce new mechanisms where necessary ensuring: (i) timely submission of accurate BO information upon registration of new LPs; (ii) timely detection and registration of changes to basic and BO information, and (iii) supervision of the accuracy and timely update of information by LPs.

IO.6 (Financial intelligence)

h) The OMLP should enhance its mechanism of prioritisation of STRs and other initiatives in line with identified risks in order to increase efficiency in operational analysis and ML disseminations originating from STRs. It should furthermore improve the existing methodology for conducting operational analysis to ensure the quality and consistency of the analyses produced.

i) The OMLP should expand its human resources capacity with requisite expertise as well as increase its technical capabilities for both operational and strategic analysis.

IO.7 (Money laundering investigations and prosecutions)

j) Slovenia should take steps to ensure that the standard of proof set by the existing and settled jurisprudence does not present an impediment in pursuing autonomous ML cases, and demonstrate effective identification, investigation and prosecution of such cases.

k) Authorities should undertake review of ML sanctions, its effectiveness and dissuasiveness, with particular focus on how delays in criminal proceedings result in lenient sanctions. Based on the findings, specific policy should be developed, with the objectives to reduce delays and ensure sanctions serve as an effective deterrent to ML activity.

l) Authorities should conduct a review across all competent authorities of the impact of the limitations on investigative powers during the pre-investigation stage of ML and associated predicate offences and address any identified deficiencies to facilitate the effective identification and development of ML cases.

IO.8 (Asset recovery)

m) Slovenia should prioritise its recent efforts to establish a dedicated asset management office to ensure the effective oversight, management and preservation of frozen and seized assets, and to support the timely enforcement of seizure and confiscation orders.

n) The competent authorities should identify and address the key impediments to the effective use of non-conviction-based confiscation and extended confiscation to ensure it can be applied effectively in practice.

o) Slovenia should address the issues of the proceeds of criminality from being returned to offenders; specifically, to prevent corporate entities or other legal persons from being abused to frustrate confiscation through offenders claiming compensation.

IO.9 (Terrorist financing investigations and prosecutions)

p) Slovenia should ensure more proactive approach to identification and investigation of TF, by employing OSINT and strategic/tactical analysis and to regularly monitor the changing TF trends and risk profile on a strategic level.

IO.10 (Terrorist financing preventive measures and financial sanctions)

q) Slovenia should establish an efficient method to communicate the UN TFS designations on TF to OEs and the general public.

r) Slovenia should (i) establish a clear reporting channel and standard form for OEs to report to the MFEA on frozen assets and attempted transactions, in line with relevant UNSCRs; (ii) designate a specific MFEA contact point to receive these reports; (iii) ensure the designated recipient has sufficient capacity (including staffing) to act on reports; and (iv) ensure all OEs are informed of the reporting form and channels.

s) Slovenia should: (i) identify the subset of organisations falling under the FATF definition; (ii) conduct an in–depth and comprehensive risk assessment of those NPOs to identify the nature of TF risk posed to them; (iii) develop focused, proportionate and risk-based measures to address TF risks and the oversight with clearly defined and coordinated responsibilities.

IO.11 (Proliferation financing financial sanctions)

t) Slovenia should establish an efficient method to communicate the UN TFS designations on PF to OEs and general public.

u) Slovenia should develop a methodology and utilise a variety of sources of information to identify, assess and understand the risk of PF breaches, non-implementation or evasion present in the country and take measures to mitigate those risks.

v) Slovenia should (i) establish a clear reporting channel and standard form for OEs to report to the MFEA on frozen assets and attempted transactions, in line with relevant UNSCRs; (ii) designate a specific MFEA contact point to receive these reports; (iii) ensure the designated recipient has sufficient capacity (including staffing) to act on reports; and (iv) ensure all OEs are informed of the reporting form and channels.

MUTUAL EVALUATION REPORT

Preface

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

This evaluation was based on the 2012 FATF Recommendations (as updated from time to time) and was prepared using the *2022 Methodology*. The evaluation was based on information provided by the country, and information obtained by the evaluation team during its on-site visit to the country from 29 September – 10 October 2025.

The evaluation was conducted by an assessment team consisting of:

- Paul NAPPER, Head of Division, Serious Fraud Office, United Kingdom
- Annette PERALES, National Coordinator Delegate, Gibraltar
- Raluca PĂTRU, Financial Analyst, Financial Intelligence Unit Romania
- Jonathan PHYALL, Head – Legal Affairs Section, Financial Intelligence Analysis Unit, Malta
- Paulis IĻJENKOVS, Deputy Head of the Financial Intelligence Unit, Latvia

with the support from the MONEYVAL Secretariat: Ana BOSKOVIC, Ani MELKONYAN, Natia JAPARIDZE and Kristina MIGGIANI.

The report was reviewed by Gordana KALEZIC (Montenegro), Alex ROWSE (Jersey) and FATF.

Slovenia previously underwent a Mutual Evaluation in 2017, conducted according to the *2013 FATF Methodology*. After the 2017 evaluation six *follow-up reports* have been published and are available at the MONEYVAL website.

That Mutual Evaluation concluded that the country was compliant (C) with 10 Recommendations; largely compliant (LC) with 19; partially compliant (PC) with 11. Slovenia was rated C or LC with 4 of the following 5 Recommendations which were triggers for enhanced follow-up during the last round: R.3, 5, 10, 11 and 20).[1]

Based on these results, Slovenia was placed in enhanced follow-up. Since its last evaluation, Slovenia achieved 12 technical compliance re-ratings:

- 9 Recommendations upgraded from PC to LC: R.1, R.5, R.6, R.7, R.8, R.13, R.26, R.28 and R.32
- 2 Recommendations upgraded from PC to C: R.12 and R.16
- 1 Recommendation downgraded from C to LC: R.15

Based on this progress, Slovenia was removed from follow up under 5th round of evaluations since all 40 Recommendations were rated LC/C at the end of the sixth follow up report.

1. For the purposes of the report, a country will be placed in enhanced follow-up if any one of the following applies: (a) it has 5 or more PC ratings for technical compliance; or (b) 1 or more NC ratings for technical compliance; or (c) it is rated PC on any one or more of R.3, R.5, R.6, R.10, R.11 and R.20; or (d) it has a moderate level of effectiveness for 6 or more of the 11 effectiveness outcomes; or (e) it has a low level of effectiveness for 1 or more of the 11 effectiveness outcomes.

Introduction to Money Laundering and Terrorist Financing Risks and Context

1. The Republic of Slovenia is located in the Central Europe. The country has a total area of 20 273 square kilometres (7 827 square miles) and population of 2 129 052 people, roughly 10% of which are foreign citizens.[2] Slovenia borders with Italy to the west, Austria to the north, Hungary to the northeast, and Croatia to the south and southeast, all countries being EU Member States. It has short strip coastline on the Adriatic Sea (46 km) which has three seaports (Piran, Izola and Koper). The capital of Slovenia is Ljubljana.

2. Slovenia is a democratic republic with a parliamentary system. The Constitution of Slovenia defines the country as a sovereign, independent, and democratic state. Slovenia's political system is based on the separation of powers among the executive, legislative, and judiciary branches. The executive branch is represented by (i) the President of Slovenia (with a rather representative and proposing role), who is elected for a five-year term, and (ii) the Government, within which the Prime Minister is the head of government and holds executive power alongside the Cabinet comprised of all the sectorial ministers. The legislative branch is the National Assembly, which is the main legislative body, consisting of 90 members. The National Council serves as the second House with 40 members, representing different interest groups (local level, employers, employees, farmers, craftsmen and independent professions, non-commercial activities).

3. The Judiciary in Slovenia is independent, with the Constitutional Court being the highest body for constitutional matters. The regular courts consist of local courts (county courts and district courts), higher courts, and the Supreme Court. The legal system is based on civil law. Primary legislation is in the form of laws and secondary in the form of regulations. International agreements require ratification by the Parliament. The Constitution stipulates that obligations imposed under ratified international treaties prevail over domestic law.

4. Slovenia is a European Union member state since 2004 and joined the EMU (Economic and Monetary Union) in 2007. The national currency is euro. It is also signatory of the Schengen Agreement since 2007.

5. Slovenia is a member of a number of 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), International Police (INTERPOL), and others.

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

Overview of ML/TF/PF Risks

6. Slovenia faces ML threats from proceeds of economic crime (abuse of office, tax evasion, business fraud) and organised crime (trafficking in drugs, weapons, people, and smuggling), classic property crime (mainly relating to online fraud and attacks on information systems), and corruption. The overall assessment of the external threat arising from cross-border crime and the activities of foreign nationals is

2 According to Statistical Office of Slovenia as of 1 January 2025 out of 10% of foreign citizens 77.2% are from the former Yugoslavia countries, 10% form EU Member States and 12.8% from other countries.

assessed as medium.

7. No terrorist acts were committed in Slovenia in the period under the review and the threat of terrorism financing (TF) is rated as low. Nonetheless, due to Slovenia's geographic proximity to the Western Balkans, and isolated cases of these countries being involved in activities in conflict zones such as Syria, Slovenia identified a potential risk of TF through the abuse of NPOs in its 2025 NRA.[3]

8. Proliferation financing risk assessment assesses risk as low[4] (see also Chapter 11). Slovenia has no direct exposure to sanctions on North Korea (DPRK), there being no diplomatic or trade relations between the countries. While no citizens of North Korea reside in Slovenia, and vice versa, during 2020-2025, no banking transactions occurred between Slovenia and North Korea.

9. Views regarding the reasonableness of the conclusions of risk assessments and on additional risks and factors which are considered significant but have not been actively taken into account are set out under Immediate Outcome 1.

Country's risk assessment & Scoping of Higher Risk Issues

10. As part of the EU, Slovenia is covered by the Supernational Risk Assessments carried out by European Commission (EC) in 2019 and 2022 and contributed to their development.

11. In the period under the review, Slovenia completed two national risk assessments (the 2021 NRA based on data from 2016-2019, and 2025 NRA based on data from 2020-2023). Both NRAs were developed through an inclusive process within the format of the Interministerial Working Group (IWG) and its 7 subgroups tasked to conduct NRAs every four years with inputs from representatives of competent authorities, including prosecutors, law enforcement authorities (LEA), supervisors as well as private sector. Both NRAs were conducted using the World Bank Methodology and utilised the findings of the EU SNRA to compare the level of risks of Slovenia against the EU. The 2025 NRA includes the PF risk assessment and an assessment of risk presented by legal persons and virtual asset service providers (VASP).

12. The AT identified the following areas of particular interest:

- Understanding of the current ML/TF risks, trends and vulnerabilities with the particular focus on how ML/TF risks have evolved since the last national risk assessment, given that the assessment relied on data from 2023. In addition, given that there was no previous assessment of potential breaches, non-implementation or evasion of UN TFS on PF the AT examined the reasonableness of their assessment and overall understanding. The change of the landscape of the ML/TF risks associated with the legal persons and arrangements was given particular attention due to the limited assessment under the NRA.
- The effectiveness of domestic cooperation and coordination to determine the exchange and coordination of information concerning the development and implementation of AML/CFT/CPF policies to conclude on the adequacy of those with the current risks.
- The authorities' capabilities to properly detect, investigate and prosecute ML and achieve convictions and support asset recovery. The results were assessed versus prominent threats. The particular interest was given to: (i) the 2024 legislative amendments limiting the possibility to use certain investigative measures; (ii) limitations identified in the previous MER including the absence of prioritisation of ML investigations and uncertainties on the evidentiary threshold

3. 2025 NRA, p.14
4. 2025 NRA, p.14

required to prove ML offence; and (iii) the issues related to the efficiency of the judiciary.

- The extent to which the TF activities are identified and investigated given that previously identified legislative deficiencies related to the scope of TF offence were rectified.
- The operation of the OMLP (the FIU of Slovenia) including (i) its independence (ii) possibilities to abuse its powers to target political parties, journalists due to some political developments that affected the OMLP's ability to function autonomously. The AT examined the impact of the issue and mitigating measures applied to limit the impact of these factors on the OMLP's ability to properly detect ML/TF cases.
- The extent to which the use of VAs and related service providers present a ML/TF risk in Slovenia given that this sector has experienced notable growth and change in regulatory framework in the period under the review.
- In the light of the NRAs and supervisory findings: (i) banks' abilities to effectively mitigate the ML/TF risks through risk understanding and application of risk-based internal controls and preventive measures, including the effective implementation of group-wide policies and procedures; and (ii) supervisory response to timely identification of weaknesses in the system, including fit and proper assessments for detection of criminals and their associates, and application of corrective measures.
- Considering a number of issues identified in the previous MER: (i) market entry and supervisory efforts, including collaboration between the OMLP and the sectoral supervisory authorities and SRBs; (ii) awareness and effective implementation of preventative measures by the DNFBPs; (iii) supervisors' understanding of risks and risk understanding by the respective DNFBPs.
- The extent of the abuse of legal persons given that they regularly feature within the context of proceeds generating crimes. The focus was on the effectiveness of mechanisms aimed at ensuring the transparency of legal persons in Slovenia, and the extent to which accurate and up-to-date basic and BO information from various sources (public and private sectors) was available to competent authorities on a timely basis.

13. The AT identified the following area of decreased focus:

- Postal money orders services because they were characterised as a low risk for ML/TF due to the following factors: (i) 100% state ownership; (ii) services being provided only to parties with a domestic address; (iii) transactions limited to domestic only and limited to EUR 1000; to (a) the gradual but constant decrease in postal money orders issued each year; and (b) the low average value of postal money orders issued each year.
- Auditors because they were found to pose low ML/TF risk due to the: (i) nature of provided services and a domestic focus; (ii) presence of the regulatory framework, regular supervision, and a good level of implementation of the AML/CTF measures.

Materiality

14. In 2024, Slovenia's GDP was 66 968 billion EUR, the GDP per capita reached 31 490 EUR, representing 92% of the EU average.[5] The services sector remains the key part of the Slovenian economy, showing growth over the last ten years, especially in the information and communications technologies, financial and commercial services, retail businesses and tourism. In 2023, Slovenian exports of goods

5. Republic of Slovenia- Statistical Office https://www.stat.si/statweb/en/field/index/1/29

amounted to 41.2 billion EUR while export of services reached 11.8 billion EUR, the total of 53 billion EUR represents approx. 91% of the country's GDP. The primary export destinations are Switzerland, Germany, Italy, Croatia, and Austria.[6]

15. According to the ECB study from December 2022, cash accounted for 73% of payments at bricks-and-mortar points of sale. While according to the ECB study from December 2024, Slovenia is facing a gradual decline in the use of cash[7] it still represents one of the countries in the EU with highest level of cash usage.

16. In 2024, the estimated share of the shadow economy in Slovenia reached 24% of GDP (mainly in hospitality, tourism and construction), while the EU average was 17.3%.[8]

17. Slovenia has a free port zone located in Koper, at the Port of Koper. Port of Koper is handling around 23 million tonnes of maritime cargo which is 3% higher compared to 2023.

Financial sector, VASPS and DNFBPs

18. Slovenia is not an international or regional financial centre. It is not a company formation centre either.

19. Slovenian financial sector is strongly integrated into the European single market, supported by the mutual recognition principle, which enables financial institutions from other EU or European Economic Area (EEA) Member States to establish a presence or conduct activities in Slovenia without needing further authorisation from the Slovenian authorities—commonly referred to as the "European passport".

Table 0.1: Number and size of financial sector – 31 December 2024

A- Type of Entity - to be listed in descending order of size	B- Number operating	C- Number registered or licensed	D – Materiality of sectors
Banks[9]	14	14 (Authorisation by ECB/BoS and National Competent Authority in Member State)	Total no. of clients: 2 567 237; Total assets: 54.2 billion EUR
Payment Institutions (PIs)	2	2 (Authorisation by BoS)	Total no. of clients: 109 409 Turnover: 359.3 million EUR
Money or value transfer services	0	0	0
Agent of foreign Money transfer service	1	1 (Authorisation by National Competent Authority in Member State)	Total no. of clients: 61 000 Turnover: 55.2 million EUR
Issuing or managing means of payment (Includes electronic money institutions and postal remittance)	3	3 (Authorisation by BoS)	Total no. of clients: 278 200 Turnover: 182.4 million EUR
Agent/Distributor of foreign EMI	3	3 (Authorisation by National Competent Authority in Member	No data available

6. https://oec.world/en/profile/country/svn
7. https://www.bsi.si/en/media/posts/ecb-study-most-of-our-payments-are-made-with-cash-but-we-use-electronic-payments-when-making-larger-purchases
8. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-economic-surveys-slovenia-2024_37e8dc60/bc4a107b-en.pdf
9. The term "banks" includes credit institutions.

		State)	
Lenders/leasing	49	49	No data available
Issuing or managing means of payment[10]	No data available	No data available	No data available
Financial Instrument Market Sector	5 investment firms (4 domestic securities firms and 1 foreign branch from member state) 51 AIFM (alternative investment fund managers) 5 UCITS (undertakings for collective investment in transferable securities) management companies authorised by the SMA	5 (Authorisation by the SMA) 11 (Authorisation by SMA) 5 (Authorisation by SMA)	Total no. of clients: 19 147 Total assets: 2 571 398 699.92 Total no. of clients: 1 084 Total assets: 845 774 880 Total no. of clients: 554 162 Total assets: 6 265 183 943
Life insurance companies	9	9 (Authorisation by ISA)	Total no. of clients: 900.043 Total assets: 8,159.7 million EUR
Life insurance intermediaries	1.352	1.470 (Authorisation by ISA)	No data available
Pension companies	4	4 (Authorisation by ISA)	Total no. of clients: 233.694 Total assets: 1,839.6 million EUR
Life insurance branches	3	3 (Authorisation by National Competent Authority in Member State)	No data available
Exchange offices	9	9 (Authorisation by BoS)	Total no. of clients: No data available Turnover: 16,5 million EUR
Virtual Asset Service Providers (VASPs)	9	35 (Registration by OMLP)	Total no. of clients: No data available Turnover: 25,5 million EUR

20. The AT ranked financial sectors based on their relative importance in Slovenia as follows: extremely important for banks; very important for EMIs, PIs and VASPs; moderately important for financial instrument marker sector; and less important for the insurance sector and other FIs. This approach was applied throughout the evaluation and was also used in the weighting of strengths and weaknesses related to effectiveness, aimed at informing conclusions and overall ratings. Data on the size of the sectors are available for different periods and are confirmed by the authorities.

Extremely important sector

21. Slovenia's financial sector is *bank-centric*; it consists of 14 credit institutions (9 banks, 3 saving banks and 2 foreign branches from other EU Member States) with total assets of EUR 54.2 billion at the end of 2024. Out of 9 banks 5 are subsidiaries of foreign banks (from the EU member states) and 4 are domestic ones. One of the important domestic banks has subsidiaries in a number of countries in the region. The total number of customers in the banking sector at the end of 2024 was 2 567 237, of which 90% were retail customers. The total number of PEPs was 1 762, which was 0,07% of all customers. There were 40 992 non-resident customers, which was 1,67% of all customers.

22. The 5 largest banks have almost 80% of the market share (taking into account the total assets) and their share in the GDP amounts to approximately 63%. Three of those are subsidiaries of EU banks (two from Italy, one from Hungary), one is a domestic bank. They are all universal banks, with the largest two

10. Includes electronic money institutions and postal remittance.

(accounting for almost 60% of the banking sector) focusing on retail banking. The smallest of the 5 largest banks is a state-owned export and development bank.

23. The 2025 NRA identified a medium-high ML/TF residual risks level for the banking sector, and the inherent risk has been assessed as increased.

Very important sectors

24. Electronic money institutions, weighted as very important sector, consists of three entities registered in Slovenia and licenced by BoS to provide electronic money issuance services (hereinafter: domestic EMI). At the end of 2023, domestic EMIs had 278 200 customers, and carried out 3.1 million transactions in the total amount of EUR 182.4 million. In the period 2020 - 2023, domestic EMIs did not offer services outside of Slovenia, despite the fact that two of the three are notified to provide electronic money issuance services in other Member States. In that period, none of the domestic EMIs operated through distributors or agents.

25. In addition, there are three foreign electronic money institutions registered in EU Member States and operating in Slovenia. All three have a license from a foreign supervisory authority to provide electronic money services (hereinafter: foreign EMIs). Foreign EMIs in Slovenia distribute and redeem electronic money on their own behalf through one or more distributors. Based on available data (one out of three reported on number of users/customers and all three reported on the volume of operations), foreign EMIs had a total of 8 589 customers in Slovenia at the end of 2024 and carried out 0.17 million transactions in the total amount of EUR 28.57 million.

26. The 2025 NRA identified a medium-high ML/TF residual risks level for the EMI, and the inherent risk has been assessed as moderate.

27. Payment Institutions sector, weighted as very important sector, consists of two payment institutions established and operating in Slovenia. These are licensed by the BoS. The two domestic PIs have 109,409 customers with an annual turnover of total amount of EUR 359.3 million. The 2025 NRA finds that the risk in this sector is increased by the possibility of making cross-border payments and the possibility of settling liabilities from an account abroad, as well as the relatively high limit defined on the credit card transactions.

28. The 2025 NRA identified a medium-high ML/TF residual risks level for the Payment Institutions sector, and the inherent risk has been assessed as moderate.

29. VASP sector, weighted as very important, consisted of 35 VASPs registered in Slovenia until July 2025. The number of registered VASPs doubled from 2022 to 2024. According to the BoS analysis, nine VASPs were actively providing services while the others did not provide services related to virtual currencies. Starting from 1 July 2025, with the enforcement of EU MiCA Regulation, only three VASPs applied for re-registration, of which two were granted and one was refused the authorisation. Other VASPs ceased activities.

30. While current volume of business is not available, in 2023, the total volume of business related to the exchange of virtual currencies into fiat currencies and vice versa amounted to approx. EUR 25.5 million. The majority of the aforementioned business (96%) was carried out by four registered virtual currency service providers. Out of a total of nine providers, five (5) also enabled exchanges from virtual currencies into virtual currencies, and the total volume of this business amounted to approx. EUR 1.4 million. Within the scope of business with virtual currencies, BTC, ETH, USDT and USCD dominated.

31. The 2025 NRA identified a high ML/TF residual risks level for VASPs, and the inherent risk has also been assessed as high.

Moderately important sector

32. Financial instrument marker sector weighted as moderately important consists of 5 investment firms (of which 1 is a branch of a firm from a Member State), 5 UCITS management companies and 51 AIFMs (alternative investment funds managers).

33. At the end of 2024, the liable entities included in the Financial Instruments Market Sector managed a total of EUR 31 578.02 million in client assets, and in that year, clients carried out EUR 4 422.01 million in transactions within the framework of the services provided by the liable entities.

34. The 2025 NRA identified a medium low ML/TF residual risks level for all investment market entities, and the inherent risk has also been assessed as medium low except for AIFS as medium.

Less important sector

35. Life insurance sector is weighted as less important sector among FIs consists of nine insurance companies licensed to carry out insurance business in the life insurance group and four pension companies. There are four groups operating in Slovenia whose parent company is registered in Slovenia. In addition, some insurance companies are part of groups whose parent company is headquartered in the EU Member States.

36. In 2024, insurance companies and pension companies accounted for EUR 2 301.6 million in gross premiums, which is 13,53% less than in 2023. Of this, EUR 1 765.3 million was accounted for by non-life insurance premiums and EUR 536.3 million by life insurance premiums. Total balance sheet of insurance companies and pension companies amounted to EUR 9 999.3 million on 31 December 2024 (insurance companies EUR 8 159.7 million, pension companies EUR 1 839.6 million) and increased by 9.86% compared to the previous year.

37. The 2025 NRA identified a low ML/TF residual risks level for insurance sector, and the inherent risk has also been assessed as low.

38. Slovenian DNFBP sector is characterised by dealers in precious metals and stones (DPMS) (1.5% of GDP), accountants and tax advisors (0.6%-1% of GDP), covered lawyers (0.2% of GDP). The other sectors, such as notaries, the real estate sector, gambling sector and TCSPs having a smaller share in the GDP, per descending order of materiality of DNFBP sectors.

Table 0.2: Number and size of DNFBP sector – 31 December 2024

A- Type of Entity - to be listed in descending order of size	B- Number operating	C- Number registered or licensed
Casinos	35	35
Real estate agents	In December 2024, the Market Inspectorate found out that 910 business entities are performing business or potentially performing business as a real estate company.	There are 2 806 real estate agents listed in the directory of real estate agents.
Dealers in precious metals and stones	In December 2024, the Market Inspectorate ascertained that 1389 business entities are performing business activity or potentially performing business activity as a trader in precious metals and precious stones or products made from these materials.	No registration/licensing needed
Covered Lawyers[11]	NA	- 1.913 attorney, - 12 foreign - 319 attorney firms

11. Refers to the ones registered with the Slovenian Bar Association.

Notaries	87	87
Auditors	48/116	48/169
Accountants	Cca. 5.000	No license needed
Tax Advisers	No data available	No license required
Trust and company service providers	NA	NA

39. The DNFBP sector is weighted the following way: extremely important for Real Estate and Lawyers, very important for Tax advisors, accountants, and dealers in precious metals and stones; moderately important for Casinos and Notaries; and less important for Auditors.

Extremely important sector

40. Real Estate, as extremely important DNFBP sector, consists of 2 806 real estate agents (natural persons), licensed by the Ministry of Solidarity-Based Future. Real Estate entities (business entities or licensed natural persons with sole proprietor status) are permitted to operate only if they employ at least one licensed real estate agent. The register of these business entities is maintained by Slovenian business registry. Out of 1100 registered entities, the Market Inspectorate found out that 910 business entities are performing business. Compared to the data from the previous assessment period, there is a trend of increasing licensed real estate agents.

41. The revenues of business entities that carried out real estate brokerage as their main activity amounted to EUR 87.87 million in 2023, or 0.14% of GDP. In the current assessment period, the revenues of real estate agents are relatively stable in terms of the share of GDP and do not deviate drastically from the previous period, in which the volume of annual turnover was estimated at EUR 70 million.

42. As acknowledged in the 2025 NRA and evidenced through criminal case discussions, the real estate sector is considered attractive for money laundering, as large sums of illicit money and are legalised through investments in real estate. Whilst notaries and lawyers may be involved in real estate transactions, it is not compulsory. Therefore, the real estate sector is identified to pose a medium ML/TF level for the inherent risk.

43. Lawyers consist of attorneys registered by the Slovenian Bar Association (SBA) (further referred in the MER as covered lawyers) and other legal advisors who are not regulated or licenced. Net revenues of the covered lawyers amount to EUR 128.65 million or 0.2% of GDP in 2023. In the current assessment period, the revenues of covered lawyers are stable. The 2025 NRA notes that in the absence of TCSPs within Slovenia, company formation primarily falls with law firms, in addition to business transactions, real estate operations, management of client funds, and the drafting or execution of contracts. These services are particularly vulnerable when combined with cross-border elements, complex ownership structures, nominee arrangements, or dealings involving foreign BOs. The 2025 NRA recognises that these activities facilitate both the placement and layering phases of ML.

44. This sector is weighted as extremely important due to the unregulated legal advisors, for which there is no available data on the size and materiality. Those that are present in the market provide a variety of legal services which include also services falling under the FATF standards. Slovenia acknowledges within its 2025 NRA that legal advisors may provide services largely similar to those offered by attorneys, including services caught under the APMLTF-2 and therefore fall within the scope of the FATF Standards. However, authorities demonstrated an inconsistent understanding of the specific activities actually provided by this group. As a result, it remains unclear whether legal advisors routinely carry out activities that fall within the FATF Standards. This uncertainty stems from the lack of information available and the absence of a comprehensive assessment of the sector, which also affects Slovenia's ability to determine

whether this group should be subject to market entry controls or supervision. The 2025 NRA notes that supervisory responsibility falls with the MIRS, though Slovenia's legal framework is not clear on this matter and, more importantly, a supervisory framework for this sector has not been implemented in practice. The 2025 NRA notes a substantial shadow market of unregulated legal advisors, creating a systemic regulatory gap and risks.

Very important sectors

45. Tax advisors and Accountants do not require to be registered for the provision of their services. In addition, licensing is not regulated by law and is left to professional organisations but membership in these organisations is not mandatory. The estimate number of those entities is between 4 000-15 000 entities (based on the business registry information). Overall, the 2025 NRA portrays tax advisors and accountants as sectors with moderate exposure to ML risk, mainly due to regulatory gaps, opacity of market participation, and the nature of services that can enable laundering through corporate structures and financial reporting**.** Given the activities that they are performing fall within the scope of FATF standards, they are weighted as very important sector. The 2025 NRA is also vague in concluding on the level of inherent risk (rated as "common risk").

46. Within the dealers in precious metals and stones (DPMS) sector those dealing with precious stones or in raw precious materials are not licenced. Other dealers in precious metals (except when dealing with raw materials) that are licenced have weak market-entry requirements. As a result, the authorities cannot determine how many DPMS are active, nor their scale of operations, client base, or product type. This opacity presents a structural vulnerability, as the sector may include informal operators, small merchants, and unregistered dealers. These significant regulatory deficiencies prevent the appropriate monitoring of the sector. There are examples of transactions being carried out with virtual assets and higher risk country. The estimated number of DPMS, per NRA, is 170 to 280. The net sales revenues of companies engaged in wholesale trade in metals in 2023 EUR 1 795 338 or 1.24% of GDP.

47. The 2025 NRA identified a medium high ML/TF level for the inherent risk.

Moderately important sectors

48. In Slovenia casinos are operated on the basis of concessions granted by the Government. There are 35 casinos operating in Slovenia with an annual gross revenue of 278.2 million. EUR. The sector is relatively material among the DNFBPs but it is also characterised by an adequate regulatory and supervisory framework.

49. The 2025 NRA identified an insignificant or low ML/TF level for the inherent risk.

50. In Slovenia Notaries are licensed by the MoJ and have a mandatory membership with the Notary Chamber of Slovenia. There are 87 notaries operating in Slovenia. The annual gross revenue is around 29.44 million EUR. Notaries, among other services are engaged in validation of the transfer of the real property and the sale of companies (including the transfer of shares), both being recognised in Slovenia to be systematically abused for ML purposes. The sector is characterised by a weaker supervisory framework.

51. The 2025 NRA identified an increased ML/TF level for the inherent risk.

Less important sectors

52. In Slovenia audit services may only be provided on behalf of an audit firm by persons who are licensed to perform the duties of a certified auditor. An audit firm must have a license from the Agency for Public Oversight of Auditing. There are 48 licensed audit firms and 116 licensed natural persons. In 2023 the annual gross revenue of audit firms amounted to EUR 45.5 million or 0.072% of GDP.

53. The 2025 NRA identified an insignificant or low ML/TF level for the inherent risk.

Legal persons and legal arrangements

54. In Slovenia, legal persons are divided between ‘business entities’ and ‘entities having no equity’. Business entities include the unlimited liability company (d.n.o.), limited partnership (k.d.), the limited liability company (d.o.o.), the public limited company or joint-stock company (d.d.), the limited partnership with share capital (k.d.d.), cooperatives and branches of foreign companies. Entities having no equity would cover the economic interest groupings (GIZ), institutes, foundations, political parties, trade unions, religious communities, associations (or societies) and branches of foreign associations. Only foundations for public or charitable purposes can be established in Slovenia.

55. As of end December 2024, there were a total of 109,420 legal persons registered in Slovenia. Among business entities, the most common form of legal person is the limited liability company, which accounts for 70% of all registered legal persons. By contrast, the second largest group of business entities (joint stock company) accounts for about 0.3% of all legal persons registered in Slovenia. As regards entities without equity, associations are the highest in number, constituting about 20% of all registered legal persons.

56. Legal persons registered in Slovenia are not usually characterised by complex ownership and control structures. The percentage of companies where legal ownership is exercised through other legal persons and/or arrangements is quite contained, the highest being an average of 13% in the case of limited liability companies. On the other hand, foundations present a higher percentage at around an average of 42% over the assessment period.

57. Register of Beneficial Ownership has been in place in Slovenia as of December 2017. While all legal persons and branches of legal persons present in Slovenia are required to disclose BO information thereto, currently 81,191 legal persons have been entered into the BO register, which falls short of the total number of legal persons. About 80% of 293,041 individuals registered as BO are Slovenian nationals or residents. The greatest concentration of foreign BOs is associated with limited liability companies, with 25% of all registered BOs being foreign residents. Foreign BOs are mostly resident within the Balkans or Central Europe, exception being made for a significant cohort that are resident in China.

58. Legal arrangements are not recognised under the laws of Slovenia. However, foreign trusts that are managed or administered from Slovenia are subject to disclosure requirements both with regards to basic information as well as beneficiary information. Foreign legal arrangements do not seem to be active in Slovenia.

Structural Elements

59. Slovenia has political stability, government, rule of law and judiciary. Since gaining independence in 1991. Slovenia has maintained a relatively stable governance environment, with a focus on economic development, democratic principles, and the protection of human rights. Hence, the structural elements needed to ensure an effective AML/CFT system are present.

60. As a member of the EU, Slovenia applies EU law. EU Regulations are directly applicable, while EU Directives are transposed through domestic law.

Background and other Contextual Factors

61. Slovenia has mature AML/CFT regime and institutions that are implementing it. There is also mature regulatory, supervisory and administrative regime in the country.

AML/CFT/CPF strategy

62. There is no national AML/CFT Strategy. Instead, risk assessments are complemented by ML/TF action plans. In 2021, after the adoption of the 2021 NRA, the OMLP adopted a strategic plan for 2021-2026 which primarily focuses on its own institutional objectives and therefore cannot be considered as a comprehensive national AML/CFT policy applicable to all authorities. The 2025 NRA has its own action plan which sets out certain policy initiatives, which largely address identified ML risks. 2021 and 2025 action plans do not include particular CFT measures as TF risk is assessed low, and hence the authorities consider it well-mitigated.

63. Certain elements of AML/CFT prevention, coordination and cooperation are included in the "Resolution on National Program of preventing and fighting against Crime 2019–2024 and 2024-2028" (adopted in 2019 and 2024 respectively). The prosecution strategy as well as the counterterrorism strategy contain general references to CFT.

64. There are no national CPF strategies or policies. While the 2025 NRA includes some analysis on PF, its action plan does not address it. At the same time the MFEA had issued the Foreign Policy Strategy of the Republic of Slovenia in December 2024, which reinforces the commitment of the country to continue advocating for non-proliferation of weapons of mass destruction.

Legal & institutional framework

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

66. The Permanent Coordination Group for Prevention, Detection and Prosecution of Money Laundering and Terrorist Financing (Group) has a coordination role in streamlining AML/CFT policies and preparing National Risk Assessments.

67. The Office for Money Laundering Prevention (OMLP) of Slovenia carries out FIU functions set out in R.29. It supervises all OEs, acting as a secondary supervisor for the OEs that have their main supervisory and acting as a primary supervisor for all other OEs.

68. The Bank of Slovenia (BoS) has extensive powers to licence, register and supervise banks, MVTS and exchange offices.

69. The Slovenian Police Authority (police) is an independent agency within the Ministry of Interior. The Slovene Police is the main LEA in charge of identifying predicate offences, ML and TF.

70. The Ministry of Foreign Affairs of Slovenia (MFEA) 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.

71. 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 Specialised State Prosecutor's Office (SPO) prosecutes serious criminal activities in the areas of organised and economic crime, terrorism, corruption and other criminal activities requiring detection and prosecution by specially organised and trained state prosecutors. The jurisdiction of the SPO 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.

72. 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).

73. The Ministry of Justice of Slovenia (MoJ) is the central authority in the provision of mutual legal assistance (MLA). 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).

74. 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.

75. The Commission for the Prevention of Corruption (CPC) is an independent administrative body with a mandate to prevent and investigate corruption. It does not have law enforcement powers.

76. The Slovenian Intelligence and Security Agency (SOVA) is the central civilian intelligence and security service responsible for the protection of national security. SOVA acquire and analyse information as part of TF and counter-terrorism investigations. SOVA has also the power to request the OMLP to collect information on a particular case.

77. Supervisory Authorities: APMLTF-2 designates the institutions which carry out AML/CFT supervision of financial institutions and DNFBPs including the: BoS, SMA, Insurance Supervision Agency (ISA), the FARS, TARS, MIRS, Agency for Public Oversight of Auditing (APOA), SBA and Chamber of Notaries of Slovenia (CNS). An analysis of the functions and remits of the supervisory authorities can be found under R.26-28.

Preventive measures

78. The AML/CFT Directive[12] sets out AML/CFT preventive rules, including the scope of obliged entities, provisions on the assessment of risks, CDD measures and record keeping requirements, beneficial ownership transparency requirements, reporting obligations, as well as the powers and tasks of FIUs and supervisors and information exchange and cooperation between authorities.[13] Traceability of fund and

12. Directive (EU) 2015/849 as amended by Directive (EU) 2018/843 (the "5th AML/CFT Directive").
13. A new Regulation and Directive came into force (but not effect) on 9 July 2024 and Directive (EU) 2015/849 will be replaced as follows:
Regulation (EU) 2024/1624 (the "EU AML/CFT Regulation"), covers all preventive rules, including by setting out the scope of obliged entities and the rules that apply to their internal AML/CFT systems, CDD measures, record keeping requirements, reporting of suspicions to FIUs, as well as beneficial ownership transparency and mitigation of specific risks stemming from anonymous instruments such as bearer shares/share warrants, cash and anonymous accounts. The AML Regulation shall apply from 10 July 2027, except for certain provisions relating to professional football clubs and football agents which will apply on 10th July 2029.
Directive (EU) 2024/1640 (the '6th AML/CFT Directive') sets out the power and tasks of FIUs and supervisors and creates structures for cross-border cooperation and information exchange between authorities. It also includes provisions on the assessment of risks, including a direct obligation on the Commission to assess risks at Union level every 4 years

crypto-asset transfers are regulated under Regulation (EU) 2023/1113 (the “Transfer of Funds Regulation” (TFR)).

79. Act on the Prevention of Money Laundering and Terrorist Financing (APMLTF-2) was adopted on 23.03.2022 and had undergone amendments in November 2022, March 2025 and July 2025. It transposed into the Slovenian legal framework the EU Directives from 2015 and 2019 and a number of other EU regulations. It sets the obligations of obliged entities.

80. The preventive framework in Slovenia is broadly in line with the requirements of the FATF standards. However, compliance is affected by: (i) the level of adequacy of the risk assessment of various sectors, such as legal persons and arrangements, NPOs, VASPs, etc.; (ii) the lack of licensing regime for the Tax Advisors, Accountants, DPMS dealing in precious stones and precious raw metals; (iii) insufficient understanding of legal advisors’ activities that provide services as under c.22.1(d).

81. At the same time, as concerns the scope of application of the preventative measures, it should be also noted that traders in precious metals and stones are considered to be OEs (APMLTF-2, Art.4(1),19(m)) and therefore are obliged to apply CDD measures. They are also prohibited from accepting cash payments over EUR 5 000 whether in one or multiple payments (linked transactions) (APMLTF-2, Arts.74(1) and 74(2)) and payments in other currency than Euro (Euro Introduction Act Official Journal of the Republic of Slovenia, no. 114/06). Thus, c.22.1(c) is not applicable for traders in precious metals and stones since the FATF Standards envisage the threshold of cash transactions is EUR 15 000.

82. Slovenia published a Decree on the exemption of organisers of classic games of chance from the implementation of AML/CFT measures which was rated as low risk in the NRA (APMLTF-2, Art. 9 and Art. 190(2)). The adoption of the Decree was based on a specific risk assessment conducted by the FARS in cooperation with the OMLP.

83. Slovenia allows specific exemptions from the application of AML/CFT measures for legal entities, sole traders and self-employed persons (APMLTF-2, Arts. 4(1)(15), 4(19)(a)-(g)) who carry out financial activities on an occasional basis, ancillary and directly related to their main activity when there is proven low risk and subject to certain conditions (Art. 11 APMLTF-2).

Supervisory arrangements[14]

84. The AML/CFT/CPF supervisory authorities in Slovenia are designated under provisions of Article 152 of the APMLTF-2 and Article 10 of Act on restrictive measures (ARM).

85. Supervision of financial institutions is conducted by the Bank of Slovenia, Securities Market Agency, Insurance Supervision Agency and Market Inspectorate of the Republic of Slovenia.

86. Supervision of DNFBPs is conducted by Financial Administration of the Republic of Slovenia, Market Inspectorate of the Republic of Slovenia; the Agency for Public Oversight of Auditing; the SBA and the CNS.

87. The OMLP is designated as a secondary supervisor for all those entities which have their primarily supervisors. It is acting as a primarily supervisory for the OEs which do not have designated supervisory

(and more frequently as needed for specific risks) and on beneficial ownership registers, including directly applicable provisions regarding their interconnection. The 6th AML Directive shall be transposed by 10 July 2027, except for certain provisions related to: (i) access to Beneficial Ownership Registers which will have to be transposed earlier; and (ii) single access points to real estate data, which have a later transposition date.

14. Assessors should describe the supervisory arrangements in place for financial institutions, VASPs and DNFBPs.

authorities, such as tax advisors and accountants.

88. Registration of unlimited liability 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), European public limited liability company, limited liability co-operatives (z.o.o.), no-liability cooperatives (z.b.o.), cooperatives established in the fields of agriculture and forestry, and institutes is done by courts, while the application for the registration is filed through a notary or the online platform Slovenian Business Point (SPOT). Decision on the registration the associations and foreign association lies on local administrative units in whose area of jurisdiction an association has its head office or where an affiliate of a foreign association has its head office in Slovenia. The Ministry of Interior is responsible for maintaining the central register of associations and for the register of affiliates of foreign societies. Decision on the constitution foundations lies with different Ministries, depending on the activity to be carried out by the foundations in question. Their decisions are then communicated to the Ministry of the Interior. Ministry of the Interior file the foundation, ex-officio, in the Register of Foundations. The Ministry of the Interior is also responsible for registering political parties, whereas the Ministry of Culture registers religious communities. Registration of trade unions falls under the responsibility of the Ministry for Labour. Trusts or similar legal arrangements cannot be established under the laws of Slovenia.

International Co-operation

89. International cooperation is of a great importance in Slovenia. There are well established mechanisms for international cooperation at all levels. Slovenia is part of all important international organisations and initiatives. MoJ serves as Central authority for MLA with non-EU countries and cooperation with EU counterparts is conducted through well-established mechanism of European instruments.

Chapter 1. Assessment of Risks, Co-ordination and Policy Setting

The relevant Immediate Outcome considered and assessed in this chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this chapter are R.1, 2, 33 and 34 and elements of R.15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) During the assessed period, Slovenia has conducted two NRAs, in 2021 and 2025. The 2025 NRA provides a greater analytical scope covering different sectors, but data limitations, particularly from DNFBPs and judicial statistics, undermine its robustness. Both NRAs identify similar and ongoing vulnerabilities, including limited STR analysis, resource constraints across authorities, and weak supervision of DNFBPs.

b) Slovenia's understanding of ML is considered largely adequate and more sophisticated than that of TF. While the 2025 NRA reaffirms that ML risk landscape has not changed significantly compared to the 2021 NRA, Slovenia has not demonstrated that it has effectively understood and addressed the persistent and ongoing threats and vulnerabilities. LEAs, Prosecutors and the BoS demonstrated a better understanding of TF threats and risks and applied a more targeted approach to TF within their activities. However, most authorities justified the assessment of low TF risk primarily by the absence of terrorist activity within Slovenia and have not conducted a comprehensive evaluation that considers potential inherent threats and vulnerabilities.

c) Slovenia does not have any national AML/CFT Strategy or coordinated national objectives. The OMLP has its own strategy for 2021–2026 which focuses on its own institutional objectives. Slovenia did implement an action plan following adoption of its 2025 NRA, that sets out policy initiatives and largely addresses key risk areas, although it does not address national priorities or objectives. Moreover, some of the actions are formulated at a relatively high level and have long completion timeframes.

d) Slovenia has carried out comprehensive assessment to justify exemptions relating to the Games of Chance sector. Some other activities, such as legal advisors or dealers in precious raw metals and precious stones, remain outside the scope of the APMLTF-2 and are therefore exempt from AML/CFT obligations. Slovenia has not demonstrated that it has conducted a risk assessment to justify or support these exclusions.

e) The BoS activities are aligned with the risks identified in the NRAs. Other supervisors and SRBs, particularly in the DNFBP sectors among which only FARS has demonstrated a more developed risk understanding, have not embedded NRA findings into their activities. While having adequate understanding of risks, LEAs and judicial authorities generally act reactively in response to criminal activities and do not demonstrate a proactive approach to aligning their activities with the identified key ML/TF risks.

f) Support at the policy making level is not sufficiently demonstrated with respect to the strategic coordination of ML/TF mitigation. Slovenia does not currently have any coordinated mechanisms to monitor progress on actions arising from the NRAs; however, they have indicated that these will be implemented in the future through the Interministerial Working Group responsible for the development of the NRA. Slovenia lacks an integrated, prioritised, and adequately resourced framework to ensure that policy actions effectively address and mitigate the country's key ML/TF risks.

g) Operational coordination mechanisms exist between LEAs, Prosecutors and the OMLP concerning the adoption of special investigation teams. There are no other formal operational coordinating measures, and authorities have expressed concerns regarding shortness of expert resources available to manage the required obligations. Informal cooperation between the OMLP, financial supervisors and reporting entities is effective, but structured inter-agency information-sharing and typology exchange are limited.

Key Recommended Actions (KRA)

a) Slovenia should enhance its risk-based approach by establishing a formal national AML/CFT strategic framework through the adoption of national policies with (i) strategic priorities and measurable objectives aligned with the findings of the 2025 NRA; (ii) clear division of responsibilities and reasonable timeframes for implementation; and (iii) mechanisms for coordination, monitoring, periodic review, and reporting on progress. Furthermore, all competent authorities should establish their own strategies and policies in line with the national framework, ensuring that the findings of the 2025 NRA are systematically embedded into their operational objectives, activities, and enforcement priorities.

b) Slovenia should significantly strengthen its high-level policy coordination in combatting ML and TF by: (i) formalising working group governance arrangements and providing the groups with the relevant policy making authority, and (ii) providing the necessary resources for dedicated staff to be able to manage their required obligations.

Other Recommended Actions

a) In its next NRA, Slovenia should address the shortcomings identified in previous risk assessments, including limitations in the availability and granularity of data, as well as incomplete data collection from a number of sectors.

b) Slovenia should further assess its TF risk exposure more comprehensively, ensuring the use of comprehensive quantitative data in addition to its empirical knowledge.

c) Slovenia should assess the impact of the unregulated or partially regulated sectors that are currently exempt from AML/CFT obligations, in more detail, and implement a clear action to either justify these exemptions or take measures to bring them into scope of APMLTF-2.

d) Regarding the NRA action plan, Slovenia should introduce formalised measures to ensure the monitoring of these actions and that they are periodically reviewed to keep them up to date and adequate to evolving and emerging risks.

Overall Conclusions on IO.1

Slovenia's understanding of ML is largely adequate and more sophisticated than that of TF. Slovenia has made significant progress in identifying, assessing and understanding ML/TF risks through its successive NRAs. The 2025 NRA shows improved methodological standards, increased variety of datasets analysed, expanded coverage of sectors, greater inclusion of emerging typologies such as cyber-enabled fraud and virtual assets. LEAs still approach ML as a secondary matter to predicate offences which may narrow their risk understanding, and TF risk continues to be perceived as negligible not sufficiently substantiated by a comprehensive assessment. Slovenia lacks a national AML/CFT strategy and the absence of a mechanism to monitor implementation of successive action plans weaken its strategic approach to its ML/TF policy response.

Authorities demonstrate limited cooperation overall, however, while some level of operational cooperation exists, policy-level coordination remains significantly weaker and less developed. The Inter-ministerial Working Group and other coordination groups operate without established governance systems, and performance metrics, and insufficient senior-level authority to lead national policy efforts. Slovenia's authorities' efforts cannot fully translate into an effective, risk based national response to ML/TF risks.

Slovenia is rated as having a moderate level of effectiveness for IO.1.

1.1. Country's identification, assessment and understanding of its ML/TF risks

90. Since 2017 MER, Slovenia has made considerable efforts to improve its understanding of ML/TF risks through two successive NRAs completed in 2021 and 2025. Development of these NRAs through an inclusive process led by the OMLP with the participation of supervisory authorities, prosecutors, law-enforcement agencies and representatives of the private sector within the format of the permanent Interministerial Working Group (IWG) and its 7 subgroups has contributed to improved identification, assessment and understanding of risks. The findings of the EU SNRA being analysed and taken into consideration by the subgroups while developing the NRA also contributed to Slovenia's risk understanding *vis-à-vis* the regional supranational context.

91. While NRAs remain the main mechanism for informing Slovenia's understanding of ML/TF risks, the 2025 NRA marks a notable improvement over the 2021 NRA, offering greater granularity and a broader analytical scope. It covers different sectors and establishes clearer linkages between inherent threats and vulnerabilities across financial and non-financial sectors. The 2025 NRA aims to portray a more holistic picture of national risks by including a country vulnerability section, applying control environment scoring, and drawing residual risk conclusions, often with a comparison to the EU SNRA. Particularly noteworthy is the inclusion of a full assessment of cross border ML, cyber enabled fraud, and new activities such as virtual assets.

92. Notwithstanding these improvements, the robustness of Slovenia's ML/TF risk assessment remains constrained by structural data limitations and uneven sectoral engagement. As a result, while the overall threat landscape is broadly identified, certain elements of the assessment lack sufficient depth and evidentiary support.

1.1.1. ML risks

93. Slovenia identifies its principal ML threats with reasonable accuracy and has demonstrated

measurable improvement between successive NRAs. Both the 2021 and 2025 NRAs consistently identify economic and financial crime, tax evasion, corruption, organised crime, and increasingly cyber-enabled fraud and cross-border laundering as the main drivers of ML risk. The 2025 NRA reflects enhanced analytical depth, broader sectoral coverage and improved treatment of foreign predicate offences, virtual assets and cross-border vulnerabilities, indicating institutional learning and strengthened methodological capacity.

94. While the 2025 NRA represents a methodological improvement over the 2021 NRA, significant data limitations continue to undermine the reliability and depth of its risk assessment. Authorities acknowledged limitations in data, including inadequate record keeping by Prosecutors and LEAs or the lack of complete data from DNFBP sectors. The 2021 NRA relied on information from STRs, and other information provided by the police, and prosecutors' office. While the 2025 NRA still relies heavily on these sources, it represents an improvement as it also includes additional data collected from the financial and non-financial sectors through targeted questionnaires. The use of targeted questionnaires for data collection from 12 non-financial sectors and professions was a major novelty of the 2025 NRA process aimed at exploring deeper the vulnerabilities of the DNFBPs. However, the reliability of the assessment derived from the data collected is questionable given the low response rate[15] and incomplete data received. Furthermore, the data collected for some DNFBP sectors was high level and insufficiently detailed to support comprehensive individual or sectoral risk understanding.

95. The use of data from STRs also has its limitations given the OMLP reported backlog in the review and analysis of STRs (see IO.6). This backlog, while delaying the timely dissemination of financial intelligence to competent authorities, creates a potential information gap to identify emerging trends or typologies, and may have affected the completeness of the NRA and the risk understanding derived from it.

96. For the purposes of analysing ML threats deriving from main predicate offences, including foreign predicate offences, a comparative analysis of the datasets for the 2025 NRA and the 2021 NRA was also carried out to identify any changes in trends. The 2025 NRA also relied on information on property gains and analysis of criminal cases conducted during the IWG subgroup discussions. Overall, while this is a positive approach that enabled the identification of relevant trends, in view of limitations of the datasets used, including gaps in the data kept by Prosecutors and LEAs, the broader threat picture associated with predicate offences may not have been fully captured.

97. The 2021 NRA established a baseline understanding of Slovenia's ML threat environment and recognised that ML risks stem mainly from domestic economic and financial crime, corruption, organised crime and tax evasion. While the 2021 NRA does not explicitly use the term "foreign predicate offences", it repeatedly incorporates the concept indirectly through its treatment of external risk, foreign proceeds, and foreign offenders. However, the analytical framework used for the 2021 NRA is narrow, descriptive, and insufficiently granular to fully satisfy a risk understanding of cross-border threats.

98. The 2025 NRA retained all previously identified threats and further recognised the growing significance of cyber-enabled fraud, online investment scams, and cross-border electronic transactions as emerging ML threats. While several of the 2021 vulnerabilities persisted, new structural weaknesses were also identified, including shortcomings in the oversight of the virtual asset sector, continuing resource and expertise gaps among DNFBP supervisors, low levels of compliance among DNFBPs, and inadequate information sharing concerning foreign beneficial ownership structures. The treatment of foreign predicate

15 As the AT was informed by the Slovenian authorities, The response rate to the questionnaires varied considerably, ranging from 100% from registered attorneys (with the SBA) and casinos, to 53.5% from real estate agents, 43% from accountants and tax advisors collectively, and 38.9% from dealers in precious metals. No information on the response rate was provided for other DNFBP sectors.

offences in the 2025 NRA is visible and substantive, and provides an improved understanding compared to the earlier NRA iteration. It reflects a realistic appreciation of Slovenia's geographic and economic connectivity and the exposure to international organised crime networks, supported by factual operational data and investigative indicators. The overall ML risk for Slovenia was again assessed as medium to high, reflecting both enduring and evolving vulnerabilities despite a more complex risk environment.

99. The understanding of risks related to the use of cash has improved through the successive NRA processes. The 2021 NRA recognised cash as a major vulnerability, noting high reliance on physical currency within the country and limited restrictions on large cash transactions. The 2025 NRA utilised better cash related data, re-confirming that Slovenia is a cash-intensive economy.[16] While the domestic use of cash is seen as largely driven by economic habits rather than illicit activity, factoring in Slovenia's geographical position as a transit country between the Balkans and Western Europe, the 2025 NRA identifies risks related to ongoing exposure to cross-border laundering through cash movements. Slovenia therefore considers that the overall ML threat from cash remains significant, assessed as medium-high.

100. In line with the 2025 NRA findings, LEAs demonstrated adequate understanding of the role of cash in criminal activities paired by the use of legal persons, citing cases involving the use of cash for the purchase of property, gold, or for cross-border transfers designed to avoid detection and reporting by Slovenian banks. However, DNFBPs representing the real estate sector, covered lawyers, accountants and notaries, did not fully recognise risks related to the use of cash or admit to accepting cash payments from customers, instead relying heavily on banks to perform CDD and monitor cash deposits. It is particularly concerning that while approximately 75% of all reported cash deposits over EUR 15,000 were made to legal entities' accounts, as per the 2025 NRA,[17] sectors involved in company formation and management, such as covered lawyers, notaries, and accountants, have submitted very few STRs (see IO.6). The AT considers that this disconnect between the high volume of cash activity among legal entities and the minimal reporting by DNFBPs highlights a possible gap in the data for the detection of potential cash-related ML risks.

101. In the 2021 NRA, corruption was assessed as medium-low. The 2025 NRA identifies similar typologies and indicates some progress, reflected in Slovenia's improvement on the Transparency International Corruption Perception Index (from rank 42 in 2023 to 36 in 2024), and stronger legislative and institutional frameworks. The 2025 NRA maintains that corruption-related offences (mostly lower-level bribery or abuse of official position) continue to represent an ongoing ML threat, albeit at a medium-low level. Overall, the 2025 NRA's assessment of corruption risk is coherent and shows continuity with previous assessments. However, structural data limitations and the absence of more granular analysis constrain the ability to fully gauge the scale and evolution of corruption-driven threats.

102. LEAs, prosecutors, and financial sector representatives (both supervisors and OEs) demonstrated an adequate understanding of ML risks. Their views were broadly aligned with the risks identified in the NRAs and were generally consistent across competent authorities. In contrast, the AT observed a noticeably lower level of understanding among non-financial supervisors, who were less able to articulate sector-specific threats, vulnerabilities, and emerging trends with the FARS being the only supervisor demonstrating a more developed understanding. This discrepancy indicates that risk understanding is stronger and more developed within the financial sector than within the DNFBP supervisory landscape.

103. FIs supervised by the BoS generally demonstrated a good understanding of their ML risks,

16 2025 NRA, p.93. While the share of cash payments at points of sale (POS) declined from 80% in 2016 to 64% in 2024, this still represents one of the highest levels of cash usage in the EU. The proportion of citizens considering cash as "very important" remains at 31%, indicating continued cultural use of cash despite the increasing digitisation of payments.

17 2025 NRA, p.93. According to the 2025 NRA, out of over 400 000 reports relating to cash transactions exceeding EUR 15 000 received by the OMLP during 2020-2024, approximately 75% concerned cash deposits made to legal entities' accounts.

particularly banks and EMIs, which showed awareness of NRA findings and sector-specific vulnerabilities. Investment firms and fund sector operators were similarly aligned with the NRA. Insurance undertakings, pension companies, and intermediaries also articulated relevant sector-specific risks and mitigating measures, while leasing and lending companies demonstrated a satisfactory level of awareness. Overall, understanding of ML risks across financial sectors appears broadly consistent with the NRA and generally well-developed, with stronger awareness in sectors facing more complex or specialised risk exposures.

104. DNFBPs demonstrated a limited understanding of ML risks, including in sectors that Slovenia identifies as higher risk. Their understanding was largely confined to the contents of the 2025 NRA and they tended to repeat its conclusions rather than contextualising sector-specific threats and vulnerabilities. Risk awareness varied across sectors: covered lawyers, notaries and real estate agents did not recognise exposure within their own activities; DPMS could not articulate sector vulnerabilities; casinos showed comparatively higher awareness due to strong supervision by FARS; and accountants and auditors belonging to international groups demonstrated the most developed understanding.

105. While no other sectoral risk assessments have been conducted, other analytical activities, like Serious and Organised Crime Threat Assessment (SOCTA) conducted by the police authorities, may contribute to the overall risk understanding. As it was completed after the 2025 NRA, SOCTA's findings were not integrated in the NRA and they are yet to be shared with other authorities.

1.1.2. TF Risks

106. Slovenia's understanding of TF risks derives from the same NRA processes as for ML since ML/TF risks were tackled simultaneously by the IWG and its subgroups. The 2025 NRA found no concrete evidence of systemic TF activity, thereby reaffirming Slovenia's low exposure to TF threats. However, it did note a gradual increase in TF-related intelligence exchanges.

107. TF risk understanding has evolved through the two successive NRAs. In the 2021 NRA, Slovenia identified the main TF threats as cash couriers, the misuse of NPOs, and isolated instances of informal value transfer systems (hawala). The 2025 NRA further recognised additional emerging risks, including small-scale self-funding by radicalised individuals, the occasional use of online payment tools and virtual assets linked to conflict zones, and the potential abuse of NPOs.

108. When discussing TF, most authorities appeared to equate Slovenia's TF risk with the absence of terrorism within Slovenia and the low level of risk identified in the NRAs. There was limited recognition of potential or inherent TF threats that may exist. LEAs, prosecutors and security service demonstrated a good understanding of inherent TF threats on the examples of cases discussed during the onsite visit. Their threat assessment takes into consideration both the country and regional context. They have also put in place mitigating measures such as monitoring of groups more susceptible to radicalisation as well as observing trends in criminality (e.g. monitoring links between organised crime groups and extremist groups to detect potential risks of TF).

109. Similarly, the BoS also demonstrated a good understanding of TF threats and risks, in comparison to other supervisory authorities and SRBs, and incorporated TF specific actions into its supervisory framework. The BoS acknowledged the higher risk of TF posed by sectors such as VASPs and MSBs and ensured that as part of its supervisory activities it analysed the transactional data within these sectors to identify any potential TF. Other FI supervisory authorities, and all DNFBP authorities, demonstrated a less developed understanding of TF risks. DNFBP supervisors viewed TF and ML vulnerabilities as largely identical, without differentiating between the two. The AT considers that this reflects a need to strengthen understanding of the unique vulnerabilities associated specifically with TF. The persistent shortage of

specialised human resources further compounds this weakness.

110. The 2025 NRA demonstrates a clear advancement and improvement in Slovenia's analysis of TF risks. Nonetheless, the authorities noted an inconsistent recordkeeping and sharing of TF-related information which limited the adequacy of an overall national risk assessment. Limited consideration of TF microfinancing risks associated with alternative financial networks, such as hawala systems, indicates that further refinement of the national TF risk picture would be beneficial. Similarly, while some NPO risk assessment has been carried out outside the NRA processes, it was not comprehensive enough for proper understanding of TF-related risks in this sector (see IO.10). Furthermore, there seems to be limited to no systematic information sharing among authorities regarding the TF risk landscape, further constraining the development of a coordinated and comprehensive national understanding of TF risks and the development of a shared TF risk understanding.

1.1.3. Dissemination of ML/TF Risk Conclusions

111. The full 2021 NRA report and summary of the 2025 NRA are publicly available. The authorities, supervisors, SRBs and private sector representatives confirmed to the AT that the 2025 NRA had been shared with them by the OMLP. Competent authorities also confirmed that the NRA is further shared with all staff within their relevant organisations.

1.2. National policies and activities to address identified ML/TF risks

112. As central authority for AML/CFT under the APMLTF-2, the OMLP is responsible for coordinating national policy. Slovenia has not adopted any formal national strategy. While both the 2021 and 2025 NRAs are accompanied by action plans intended to address higher or key risk areas, these do not amount to a comprehensive national strategy setting clear overarching priorities and objectives. The AT acknowledges that the action plans contribute to guiding national actions to some extent, however, they are largely task-focused and subject to limitations, as outlined below. As the 2025 NRA with its action plan was adopted shortly before the onsite visit, its impact on Slovenia's overall response to ML/TF risks has yet to be observed.

113. The 2025 action plan represents a structured attempt to address the ML/TF risks identified in the NRA, setting out a range of measures across institutional, sectoral, and operational levels. It assigns responsibilities and timelines to competent authorities and reflects an intention to tackle key systemic issues, including weaknesses in data collection, the absence of systematic recording of predicate offences in ML, and limitations in asset recovery frameworks. Measures such as the planned introduction of a document management system by the State Prosecutor's Office indicate recognition of important structural gaps.

114. Concerning the financial sectors, the plan targets weak CDD practices, insufficient information-sharing between the BoS and OMLP, and instances of unjustified "de-risking". Planned responses, such as legislative amendments, updated guidance for life insurance products, and strengthened oversight of virtual asset and e-money providers, are broadly aligned with the risks identified. Similarly, the plan acknowledges persistent shortcomings in the DNFBP sectors, such as ongoing regulatory and awareness gaps, and proposes measures for addressing these.

115. While the 2025 action plan demonstrates a broad alignment with key ML/TF risks and reflects a degree of strategic commitment, it presents an uneven longer term framework. Some of the actions are formulated at a high level, with significant long completion timeframes, and a reliance on legislative amendments and inter-agency coordination which have historically faced delays. Notably, key risks identified over successive NRAs are addressed through measures with relatively long timeframes, indicating

that the urgency of these risks may not be fully understood by Slovenian Authorities. For example, the regulation of accountants and tax advisors is foreseen only by 2028, despite longstanding vulnerabilities identified in these sectors since the 2021 NRA. The continued postponement of regulatory reforms for sectors already assessed as vulnerable indicates a degree of disconnect between the risks identified and the prioritisation and urgency reflected in the action plan. Taken together, the AT considers that while the action plan represents progress and demonstrates commitment, its level of specificity, sequencing, and timeliness may limit its capacity to effectively and promptly mitigate Slovenia's most significant ML/TF risks.

116. Slovenia has no existing framework to monitor progress of the 2025 action plan. The OMLP advised that it is considering extending the mandate of the IWG to include oversight of the action plan implementation, however this has yet to be put into effect. Similarly, no monitoring mechanism was applied for the 2021 action plan, limiting the Slovenia's ability to address risks in a timely and coordinated manner.

117. The AT has identified deficiencies in high-level policy coordination in Slovenia's response to ML/TF risks, arising from the lack of a comprehensive national strategy. This reflects limited systemic support at Government level for the effective implementation of mitigating measures at national level. While the working groups are comprised of experienced and committed professionals, these are not vested with relevant and sufficient authority to ensure the coordinated cross-government actions or drive the implementation of national priorities. Furthermore, authorities have not been allocated adequate level of resources to effectively address the action points. Accordingly, the AT deems that commitment at the policymaking level to address AML/CFT issues in Slovenia requires significant strengthening.

118. There are no TF-specific strategies or coordinated national objectives. Besides the analysis under 1.2.1, it should be noted that the 2021 and 2025 action plans refer to ML and TF however do not include any specific TF-related measures, as the authorities consider the TF risk to be low and well mitigated.

119. The prosecution strategy and counterterrorism strategy (the latter was not provided to the AT, but authorities advised that the strategy contains a very brief reference to CFT and its action plan foresees some CFT actions) contain general references to CFT. Certain AML/CFT elements are included in the National Program of preventing and fighting against Crime 2019–2024 and 2024-2028.

1.3. Exemptions, enhanced and simplified ML/TF measures

120. Article 14 of the APMLTF-2 sets out provisions for the use of the NRA to identify sectors or activities which require the application of stricter measures, as well as those presenting a negligible or increased ML/TF risk.

121. There are no specific exemptions, enhanced or simplified measures applied for TF.

Exemptions

122. More specifically, Art.9 of the APMLTF-2 provides for exemptions allowing some organisers of classic games of chance to be fully or partially exempt from AML/CFT measures (See R.1.7). Such exemption may only be granted following a risk assessment carried out by the FARS and the OMLP, determining that the sector poses a low risk of ML/TF.

123. This exemption was implemented by Slovenia through the Decree on the Exemption of Organisers of Classic Games of Chance, which was first introduced in October 2018, and last ratified in January 2023. The initial adoption of the Decree was based on a comprehensive risk assessment conducted by the FARS in cooperation with the OMLP, which adequately substantiated that the activities are low risk and therefore warranted the exemption, and was subsequently ratified through the NRAs.

124. Slovenia has also established under the APMLTF-2 provisions allowing exemptions for legal entities,

sole traders and self-employed persons that provide financial activities on an occasional basis or to a limited extent. This exemption is only applicable when a number of conditions are met, including that the activities are assessed as low risk. Furthermore, those seeking to benefit from the exemption must apply to the OMLP and demonstrate compliance with the conditions. The OMLP confirmed that it has not received any applications, and therefore no entities or individuals currently operate under this exemption.

125. There is also a conditional and limited exemption concerning the E-Money sector. E-Money Institutions may be exempt from certain CDD measures. Although Slovenia has not carried out a specific risk assessment to justify this exemption, it has relied on the assessment carried out under the EU Supernational Risk Assessment. Reliance on the EU Supranational Risk Assessment ensures alignment with broader EU risk findings and provides a reasonable basis for applying the exemptions.

126. Several deficiencies have been identified within R.22 whereby some activities currently may fall outside the scope of the APMLTF-2 and are therefore exempt from AML/CFT obligations. However, Slovenia has not demonstrated that it has carried out a risk assessment to substantiate these exclusions.

Simplified and Enhanced Measures

127. Slovenia's framework for enhanced and simplified measures is largely informed by the EU AML Directive, EU SNRA, and to a lesser extent from Slovenia's NRAs. However, Slovenia has not introduced additional simplified or enhanced measures that extend beyond the requirements set out in the FATF Standards and the EU AML/CFT framework.

1.4. Objectives and activities of competent authorities and SRBs

128. While Slovenian authorities advised that they had taken the identified ML/TF risks into account as part of their activities, the AT notes that this was not demonstrated in practice. With the exception of the OMLP, none of the competent authorities demonstrated that they had defined specific AML/CFT objectives, nor that the identified NRA risks had been systematically incorporated into their operational or strategic activities. As a result, authorities' actions are not consistently prioritised or guided by the key ML/TF risks identified at national level.

129. This is compounded by the absence of national strategies or policies and the lack of follow up on the action plans during the assessed period. This has resulted in an inconsistent and fragmented approach among competent authorities, with no overarching framework to ensure a coordinated and risk-based national response. The AT acknowledges the adoption of the latest action plan in July 2025 but is unable to assess its impact on changes in the authorities' operational activities.

130. The OMLP adopted its own strategy for the period 2021-2026 which included several objectives and related actions. However, the objectives are not aligned with or responsive to the key risks identified in the 2021 NRA, and the action plan derived from the OMLP's strategy lacks measurable indicators and provides insufficient detail on expected outcomes. This issue was also highlighted by the IWG, though recommendations to strengthen and update the action plan were not implemented, further limiting its relevance and effectiveness. The OMLP has not fully addressed most objectives. It indicated that it had prioritised addressing technical deficiencies before proceeding with the drafting of the 2025 NRA. The AT understood that due to resource constraints, Slovenian authorities were required to prioritise actions and were unable to address objectives concurrently. However, Slovenia lacks a framework or mechanism to monitor progress against the NRA action plans. Therefore, it is not possible to assess whether measures taken and prioritised are effectively mitigating identified ML/TF risks.

131. The OMLP's strategy has not been updated to reflect or align with the 2025 NRA, resulting in a

continued disconnect between evolving risk understanding and strategic planning. The coexistence of multiple action plans without a clear mechanism for coordination or monitoring further contributes to a fragmented approach.

132. LEAs and judicial authorities generally act reactively in response to criminal activities and do not demonstrate a proactive approach to aligning their activities with the key ML/TF risks. The State Prosecutors office adopted an enforcement policy in December 2024 covering the period 2024-2028, which identifies all categories of predicate offences, including economic crime, corruption crimes, and terrorism. While the policy provides guidance on case prioritisation within each category it does not reference or appear to align with the NRAs.

133. The absence of a strategic approach on cross-border cash movements combined with the reduced amounts detected and confiscated, specifically by the customs authorities, reflects a lack of prioritisation of this area. This is inconsistent with Slovenia's identification of high volume of cash use and with information provided by LEAs regarding the use of cash in ML cases.

134. Among the supervisory authorities, the BoS has the most developed supervisory framework and demonstrated an understanding of ML/TF risks consistent with the NRAs. However, other supervisory authorities and SRBs, while aware of the NRAs, did not incorporate the findings into their supervisory activities. Specifically regarding DNFBP supervisors, none demonstrated the application of a risk-based approach to supervision, whereby greater focus is expected to be placed on higher risk sectors and higher risk OEs, as defined by Slovenia's NRAs. This would be reflective of the lack of integration of the NRA findings and inadequate understanding of the sectors risk profiles.

135. With respect to TF, there is generally an absence of defined objectives, national strategies or action plans. Slovenian authorities primarily focus on terrorism with limited and incidental attention given to the TF component. This approach reflects the national risk assessment that TF risk is low.

1.5. National coordination and cooperation to develop and implement policy

136. Overall, the AT considers that coordination structures lack the authority, formalisation, and strategic focus required to ensure that AML/CFT policies are coherent, risk-based, and effectively implemented across competent authorities.

137. As the central authority for AML/CFT under the APMLTF-2, the OMLP is responsible to coordinate national policy. However, Slovenia does not have formal mechanisms in place to ensure effective coordination and cooperation in the development and implementation of policy. In practice, no competent authority demonstrated that coordination arrangements are used to define national policies or to ensure that NRA findings are systematically reflected in national or sectoral actions.

138. The IWG did not have formalised governance arrangements defining the scope of its responsibilities, frequency of meetings, etc. This limits its ability to function as an effective coordination mechanism capable of driving a consistent and risk-based national response. The OMLP advised that the IWG will continue to operate in the future following the adoption of the 2025 NRA, with an expanded focus on overseeing the implementation of the action plan (the update of the terms of reference of the Group is planned). The OMLP also advised that it expects to establish additional bilateral or multilateral inter-agency groups to facilitate a more structured response to emerging developments. While these proposed enhancements represent a positive and constructive step, these initiatives have not yet been implemented and therefore its effectiveness cannot yet be assessed.

139. Slovenia has other working groups (see Section 1.6) that primarily focus on operational matters,

although they may occasionally identify policy related matters. However, the participants in these groups do not have the authority to define or adopt national policy measures and such issues must therefore be escalated to higher senior officials for consideration.

1.6. National coordination and cooperation for operational purposes

140. Despite the absence of comprehensive national strategies and policies, Slovenian authorities have established a number of mechanisms for coordination and cooperation at operational level primarily through various working groups. While these groups may address ML/TF issues as part of their broader mandates, none are specifically designed to ensure coordinated AML/CFT operational matters.

141. The Working Group of the State Prosecutor's Office, LEAs and other competent authorities facilitates coordination and cooperation between the State Prosecutor´s office, the police and other competent state bodies in the detection and prosecution of offenders, resolving operational issues, establishing joint investigations teams, and addressing legislative matters. The work undertaken by the Group was acknowledged as particularly effective by both the State Prosecutor's Office and the police. Overall, the Working Group represents a constructive coordination platform that has strengthened cooperation between key authorities in practice and facilitated the handling of complex cases.

142. Working Group between Supervisory Authorities was established in 2024 with the specific purpose of coordinating voting arrangements in light of the establishment of the EU AMLA. Its mandate does not extend beyond this issue and does not encompass domestic operational coordination.

143. Permanent Coordination Group for Prevention, Detection and Prosecution of ML/TF: Its main responsibility is to exchange experiences and discuss legal issues arising from Slovenian legislation in relation to the prevention, supervision, detection and prosecution of ML/TF; and compare Slovenian legislation and court practice with those of other countries.

144. Permanent group on restrictive measures is primarily tasked with co-ordinating actions for implementing targeted financial sanctions and demonstrates a more structured approach to operational coordination. Its mandate includes the coordinating and preparing proposals for restrictive measures, facilitating the exchange of information between authorities, monitoring the implementation of adopted decisions, reporting on the effectiveness of adopted measures, and addressing legal drafting matters.

145. The Interministerial Working Group on Counterterrorism (IWGC) main tasks involve terrorist threat assessment and facilitation of coordinated counter-terrorism actions by the authorities. Led by the Slovenian Intelligence and Security Agency, its members include the police, OMLP, FARS, MFEA, the Ministry of Justice as well as the Ministry of Defence and the General Staff of the Slovenian Armed Forces. The group primarily serves as a forum for discussing emerging terrorism threats, trends and typologies, as well as exchanges of intelligence and information on concrete cases, including TF-related matters when those present themselves.

146. Besides these working groups, the OMLP has a formal signed cooperation agreement with the BoS. No formalised bilateral arrangements exist between other supervisory authorities. In practice, cooperation by the OMLP with other supervisory authorities occurs on an informal basis, primarily in relation to the joint delivery of industry training or issuance of guidance.

147. Overall, while there are some formal governance frameworks for the mentioned Working Groups, those related to their mandate, scope of responsibilities, reporting lines, decision making processes, frequency of meetings or mechanisms for monitoring implementation of agreed actions would benefit from further refining. Gaps in this respect limit Slovenia's ability to demonstrate that coordination is systematic,

sustainable and outcome orientated. In practice, coordination appears largely discussion-based rather than action-driven, with limited evidence of structured follow-up on identified policy gaps or operational issues. The absence of work plans, performance indicators, or formal reporting obligations reduced the ability of these mechanisms to drive tangible outcomes. Moreover, not all relevant competent authorities are consistently represented, and participation appears dependent on available resources rather than institutionalised arrangements. This creates a risk that coordination is reactive rather than embedded within a durable institutional framework. The AT considers that significant enhancements are required to establish the above working groups as effective cooperation and coordination mechanisms.

148. Furthermore, there appears to be a lack of regular and systematic sharing of information among competent authorities concerning typologies and emerging trends. While there have been some *ad hoc* exchanges on typologies among different authorities, the OMLP acknowledged that they lack systemic approach for identification of typologies and trends. This limited level of cooperation hinders the development of a collective understanding of ML/TF risks and reduces the overall effectiveness of efforts to identify and mitigate such risks.

149. The AT observed that the OMLP acts as the primary point of contact for AML/CFT related matters for other competent authorities, including providing advice on the interpretation and application of APMLTF-2. A similar dynamic was observed in the interaction between the OMLP and OEs. AML compliance officers of OEs maintain direct contact with the Head of the STR Department of the OMLP to coordinate actions in cases requiring potential temporary suspension of funds which are time-sensitive requiring quick action. The OMLP acknowledged that, as the suspension period for suspicious transactions is three working days, effective informal coordination has proven to be essential for rapid response from all relevant authorities to secure funds before judicial freezing measures can be applied as the latter take more time.

Chapter 2. International Co-operation

The relevant Immediate Outcome considered and assessed in this chapter is IO.2. The Recommendations relevant for the assessment of effectiveness under this chapter are R.36-40 and elements of R.9, 15, 24, 25 and 32.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Slovenia provides constructive, timely and effective cooperation to foreign counterparts on the basis of international instruments and the principle of reciprocity. The legal assistance is mostly focused on EU member states, but the authorities demonstrated that they effectively cooperate outside of the EU borders. Where a specific measure is not available under domestic law, the authorities apply a cooperative approach by providing assistance through alternative measures, ensuring that the objectives of the requests are met.

b) The competent authorities proactively seek assistance in ML cases and in relation to predicate offences when looking for evidence and offenders. These actions are broadly in line with country's risk profile. There is no comprehensive statistics on international cooperation with EU Member States which limits the country's ability to fully monitor effectiveness of this cooperation and to develop a full overview of crime trends.

c) Slovenia provides constructive assistance in asset recovery cases and has concluded one asset-sharing agreement. Competent authorities seek international cooperation to trace assets transferred abroad; however, these efforts are not fully proactive and are constrained by the requirement to demonstrate that assets remain in foreign accounts before seizure can be ordered and assistance sought.

d) Slovenian authorities have participated successfully in a number of JITs throughout the assessed period, either initiated by them or by foreign counterparts. The swift nature of this cooperation was particularly appreciated by Slovenian authorities.

e) Slovenian authorities (the OMLP, police, prosecutors, FARS, BoS) are making extensive use of informal cooperation to facilitate actions against criminality and to support supervisory actions related to ML and TF.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Slovenia should develop a tool to keep and produce comprehensive statistics on EIOs, EAWs, EFOs including information on types of predicate offences, countries of origin or destination, types of measures sought and provided, and the volume of seizure and confiscation of assets abroad or domestically based on the foreign requests to be able to monitor whether it is effectively providing and seeking international cooperation, and using all international cooperation tools in line with its risk and context.

b) Slovenia should enhance timely and proactive asset-tracing efforts by seeking the identification and seizure of assets abroad based on reasonable suspicion, ensuring that unreasonable proof that assets remain in foreign accounts does not impede the process.

Overall Conclusions on IO.2

Slovenia has an effective system in place enabling the provision of both formal and informal international cooperation. Competent authorities take a proactive approach in seeking international assistance for money laundering (ML) and predicate offence cases, broadly aligning their efforts with the country's risk profile. While legal assistance is primarily directed toward EU member states, in line with its risk profile, Slovenian authorities have also shown they can cooperate effectively beyond EU borders and apply alternative measures when specific requests are not covered by domestic law. Nevertheless, the absence of comprehensive statistics on cooperation with EU member states limits Slovenia's capacity to fully monitor whether it is effectively providing and seeking international cooperation and prevents them from developing a broader risk assessment.

Slovenia provides constructive support in asset recovery cases and has formalised cooperation through at least one asset-sharing agreement. Nonetheless, the need to prove that assets remain in foreign accounts before pursuing seizure in a foreign jurisdiction presents a practical constraint, reducing the proactiveness of asset-tracing efforts.

The country's active participation in joint investigation teams (JITs), on both an initiating and partnering basis, is noteworthy and has been particularly valued for its swift and effective results. In addition, Slovenian authorities make extensive use of informal cooperation channels to facilitate criminal investigations and support supervisory actions related to money laundering and terrorist financing.

Overall, the AT has placed great importance on Slovenia's effective cooperation and positive feedback received from global network. Yet, the development of comprehensive statistical data and further streamlining of asset recovery processes call for moderate improvements of the system.

Slovenia is rated as having a substantial level of effectiveness for IO.2.

150. International cooperation in Slovenia plays an important role in facilitating actions against criminality and criminal property. As a member of the European Union, Slovenia benefits from the free movement of goods, services, capital, and persons across much of Europe. While these advantages support economic development, they also increase exposure to cross-border criminal schemes. These, along with its geographic position on the Balkan Route, with an international port (Koper) make it attractive to criminal networks dealing with drug trafficking, migrant smuggling, arms trafficking and smuggling. Slovenia is on

the other hand not an international financial centre, nor company formation centre which is important to consider when assessing the effectiveness of the international cooperation.

151. There is a comprehensive legal framework for providing and seeking mutual legal assistance and extradition both in relation to EU and non-EU jurisdictions. Besides the national legislative regime governing international assistance in criminal matters, a considerable number of ratified bilateral and multilateral international instruments are at Slovenia's disposal when providing MLA. In instances where there is no international agreement, the principle of reciprocity is applied. In addition, authorities (LEAs, supervisors and the OMLP) have all necessary legal instruments to facilitate informal cooperation with their foreign counterparts.

152. The Ministry of Justice serves as the central authority for handling both incoming and outgoing MLA requests involving non-EU countries, whereas the OMLP serves as the central authority for the Council of Europe 1990 and 2005 Conventions for Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism.

153. Within the EU, mutual legal assistance requests are made directly between EU competent judicial authorities, through European Investigation Order.

2.1. Providing constructive, timely and quality mutual legal assistance and extradition

2.1.1 Providing evidence and locating criminals

154. Slovenia provides constructive and timely mutual legal assistance both to EU and non-EU countries and jurisdictions, and the processes and results achieved over the assessment period are further explained. The conclusions are based on the: (i) available but sometimes limited statistics; (ii) case examples; (iii) interviews held with the competent authorities; (iv) positive feedback from the international counterparts.

Providing mutual legal assistance to non-EU countries

155. All MLA and extradition requests from non-EU countries that are received by the MoJ are recorded in a case management system, with documents scanned and stored electronically. Case prioritisation is determined by the head of the unit within MoJ, with urgent matters (such as extradition, detention, searches and seizures, and transfers of sentenced persons) handled the same day. All MLA requests are forwarded to competent authorities for execution, typically within 1-2 days. The system allows extraction of statistics by case type, status, institution, and country, which is a clear improvement compared with the conclusions of the 2017 MER. Furthermore, the MoJ regularly tracks the execution of a request and undertakes follow up actions in case the request is not executed for a long time.

156. The MoJ provided statistics on the number of MLA requests received during 2020-2024 (See table 2.1).

Table 2.1. Incoming MLA requests (from non-EU countries)

Incoming MLA requests	2020	2021	2022	2023	2024	TOTAL
ML	6	3	6	6	4	25
Terrorism, including TF	0	0	0	1	0	1
Drug trafficking	15	9	10	4	6	44
Participation in an organised criminal group and racketeering	3	1	1	0	1	6
Trafficking in human beings and migrant smuggling	7	2	2	2	3	16
Sexual exploitation, including of children	4	3	3	0	3	13
Illicit arms trafficking	2	1	0	2	0	5
Corruption and bribery	1	0	0	1	5	7
Fraud	11	18	10	5	8	52
Murder, grievous bodily injury	1	1	0	1	1	4
Kidnapping, illegal restraint and hostage-taking	0	0	0	1	0	1
Robbery or theft	1	4	1	1	0	7
Smuggling (including in relation to customs and excise duties and taxes)	2	1	0	0	2	5
Tax crimes (related to direct and indirect taxes)	5	2	5	3	0	15
Extortion	0	1	0	0	0	1
Forgery	2	1	0	2	1	6
TOTAL	**60**	**47**	**38**	**29**	**34**	**208**

Source: Ministry of Justice

157. Over the period under review, the most common predicate offences for which MLA was requested were fraud, drug trafficking, human trafficking, tax crimes, sexual exploitation, corruption and bribery, theft, and forgery. Only 1 MLA request was related to terrorist financing. These is closely in line with the country's risk profile.

158. The positive feedback of the global network revealed that Slovenia consistently handles MLA requests, providing high quality assistance within reasonable time frame. Several countries noted improvements in Slovenia's cooperation. In particular, improved response time in the recent years and the constructive and efficient cooperation in cases involving organised crime and corruption have yielded significant outcomes, underscoring Slovenia's commitment to provide constructive assistance.

159. When it comes to MLA requests related to ML, all 25 of them received in the period under review were executed by Slovenia, except one from 2020, where assistance was refused on the grounds that the addressee of the documents to be served was not located within the territory of Slovenia. The predicate offences underlying money laundering in those requests included tax crimes, forgery, abuse of position or trust, fraud, smuggling, theft, corruption or bribery, and other related offences.

160. The average execution time ranged between 80 days (2020) to 110 days (2024). However, there are notable examples where assistance was rendered within just few days (see box 2.1). In addition, an MLA request involving terrorism financing received in 2020 was executed in only 30 days.

161. The duration usually depends on several factors, such as the urgency of the case, the complexity and scope of the specific request. Overall, the AT concludes that Slovenia ensures efficient execution of MLA requests, prioritise complex and urgent cases and is seen as a reliable partner in international cooperation.

Case Box 2.1: Providing timely assistance

Case example 1

On 5 January 2021, the Ministry of Justice received a request from a third state, under a bilateral treaty, to hear nine witnesses in a money laundering and organised crime case. The request was forwarded to the competent court the following day. Authorisation was granted for representatives of the requesting authority to attend the hearings, which were conducted by the Slovenian court on 9 February 2021 in the presence of the requesting state's prosecutors.

Case example 2

Late in 2022, prosecutors of Country Y submitted a MLA request to Slovenia, seeking the execution of covert investigative measures, including the acquisition of data from electronic communication networks, interception and recording of electronic communications, and covert surveillance. The case involved an organised criminal group engaged in the illicit production and trafficking of drugs across several countries, including neighbouring EU states and South America. Some suspects had temporarily resided in Slovenia, and one member was a Slovene national. A Slovenian court authorised the acquisition of electronic communications within seven days of the submission by foreign country. The SPO issued an order for covert surveillance of two suspects, with the police conducting operational activities under the SPO's direction. The evidence obtained in Slovenia was significant and contributed to the prosecution of serious criminal offences in Country Y.

162. The most common requested measures and documents included: evidence gathering (such as bank information, documents from official records, etc.), hearing of defendant and/or witnesses, service of documents, surveillance of electronic communications including interception, providing reports on covert surveillance, locating suspects, seizing CCTV footage and other objects, identification of individuals and vehicles. MLA and directly received EIOs through which banking information is requested are referred to the competent courts for execution, as such matters fall within their jurisdiction.

163. In some cases, when national legislation does not entirely provide for the measure as requested by the foreign counterparts, the authorities seek to find the most suitable solution and render the assistance. For example, in Slovenia there are some legislative gaps in applying special investigative techniques – controlled delivery. Also, covert monitoring of a transport of goods can be carried only when it concerns restricted (weapons, pharmaceuticals, etc.) or prohibited (illicit drugs) goods. Despite this, Slovenian judicial authorities demonstrated willingness and creativity to find alternative measures to provide the requested assistance even in situations involving controlled delivery of ordinary goods intended for criminal activities. (See Box 2.2). This is clear evidence of the willingness, ability and commitment of the authorities to provide constructive mutual legal assistance.

Case Box 2.2: Providing assistance in controlled delivery

In 2024, the SPO received a MLA request from a non-EU country (country A) regarding the monitoring of two shipments of truck tire inner tubes. It was stated that members of an organised criminal group were allegedly using these inflatable tubes as flotation devices attached to small boats to smuggle migrants from country X across the sea passage through Slovenia into country A.

In order to facilitate the provision of mutual legal assistance, Slovenian authorities informed country A of the applicable national legalisation and at the same time explored ways to render assistance (through ordering the surveillance of the individuals or transporters involved in the consignments). The prosecutor immediately issued an oral order for covert surveillance of the suspect, which was followed by a written order.

In the end, this measure was not executed because both suspects had not entered the Slovenian territory. Nevertheless, this case demonstrates authorities' willingness and swift engagement when cooperating with other countries.

164. The large majority of MLA requests are executed, with an average execution percentage of 90% during 2020-2024. Slovenian authorities presented several case examples, demonstrating their effective efforts to provide assistance in all instances unless the execution of the request would breach fundamental human rights or would prejudice the sovereignty and security of Slovenia. In instances where the MLAs were refused, it was based on the following grounds: (i) dual criminality when it comes to coercive measures, (ii) the requested measure could not be executed under national legislation, (iii) the execution of the request would have jeopardized a parallel pre-trial investigation in Slovenia (e.g. hearing of suspects), (iv) unavailability of evidence/addressee in Slovenia. The AT did not come across cases or instances where refusals were unreasonable. For example, for ML offence, only one MLA request was refused as the addressee of the documents to be served was not located in Slovenia.

165. The AT identified the most common challenges faced when providing MLA, namely poor translations, lack of clarity of the request or insufficient supporting documents. In such instances the competent authorities are proactive and seek further information from the requesting country to proceed with the execution of the request. The AT further examined the potential impact of the 2024 CPA amendments which raised the evidentiary threshold for ordering covert investigative measures and obtaining banking data (see IO.7 for further analysis) on the ability of Slovenian authorities to respond to foreign requests promptly. While the authorities did not conduct the comprehensive analysis, the information provided by the District Court in Ljubljana (the largest court in Slovenia with the highest case load of MLA requests and EIOs) for the years 2024 and 2025 demonstrates that EIOs and MLA seeking banking information are executed within the deadlines, without any refusals related to the increased threshold. In 2024-2025 only two requests were reasonably refused because the banks from which data was required were not located in Slovenia.

Providing assistance to EU member states

166. EU member states account for the greater proportion of formal legal assistance requests, which corresponds with Slovenia's assessed risks and geopolitical situation. Within the EU, mutual legal assistance requests are made directly between EU competent judicial authorities, through the EIOs. The Slovenian authorities provide timely and good quality assistance to their EU counterparts. This conclusion is based on the interviews, statistics and case examples.

167. The Slovenian authorities maintain statistics on incoming EIOs (see table 2.2), though the scope of the data is not fully comprehensive, as some EIOs initially received by the prosecution are forwarded to the courts for execution. In such cases, the processing status of these EIOs might not be fully captured within the available data, even when the requests have been executed. Despite this, the available data indicate that, between 2020 and 2024, Slovenian courts and prosecutors processed EIOs within an average of 2.5 months. This timeframe is considered efficient and demonstrates compliance with the deadlines prescribed by EU legislation. The data thus suggest that, overall, Slovenian authorities are able to execute EIOs in a timely manner, although efforts to improve the comprehensiveness and reliability of statistical recording would further enhance the effectiveness assessment.

Table 2.2. Incoming EIOs

Year	Received	Resolved	Average duration (months)
2020	406	305	2.08
2021	446	339	2.55
2022	390	359	3.52
2023	357	309	2.66
2024	610	461	2.26
2025*	244	N/A	N/A
Total	**2453**	**1773**	**2.61** (arithmetic mean)

*Data available for the 1st half of 2025

168. The feedback provided by the EU countries confirms Slovenian authorities are typically rapid to respond to EIOs and demonstrate a strong willingness to cooperate, successfully executing the requested measures. This is especially evident from a number of case examples provided (see example in Box 2.3.). These cases demonstrate Slovenia's operational capacity and willingness to cooperate promptly and effectively with foreign counterparts, both at the law enforcement and judicial levels. Also, it should be noted that that Slovenian judges take consistent and reasonable decisions when executing foreign requests for legal assistance, in accordance with the national laws, EU normative acts, jurisprudence of the Constitutional Court, the ECHR and ECJ. This, coupled with the below statistics and the numerous case examples presented, shows that Slovenia successfully responds to most of the EIOs received in due time, reflecting a strong commitment to providing international legal assistance.

169. There are no precise statistics on the offences for which the EIOs are received, but the practice has shown that EIOs are most prevalent in cases of fraud, drug trafficking, and thefts. The type of the assistance varies and involves requests for different actions to be undertaken in the territory of Slovenia on behalf of other EU member states. In practice, the SPO frequently receives urgent EIOs requiring rapid application of the interception of telecommunications to be carried out in Slovenia. In such cases, SPO consistently provides favourable opinions (allowing the requesting state to carry the interception of telecommunications on Slovenian territory without the technical support of Slovenia) often within 24 hours or even on the same day. For example, in one case prosecutors issued a favourable opinion regarding a ML case involving a hawala (underground banking) operation, which handled about 2 million euros in just one month. This demonstrates the prosecutor's ability to act swiftly and effectively in high stakes and time sensitive situations. Besides, Slovenian prosecutors participate in and are supported by Eurojust. This support is reflected in the quality of assistance provided through this mechanism. In some instances, the police forces of other EU member states take part together with the national police in the investigative actions undertaken in the territory of Slovenia which proved to be effective in facilitating activities against criminality.

Box 2.3: Execution of EIOs by the Slovenian authorities

In 2024, the security officer of the Port of Koper observed two individuals behaving suspiciously while diving under a moored vessel and promptly informed police. Police officers detained the two divers and conducted a thorough search. The search resulted in the discovery of several packages of cocaine clandestinely attached to the vessel's structure. Criminal investigation was initiated for drug trafficking and subsequently it was revealed that the case had a transnational element: citizens of two other countries were also involved and the suspects had used vehicles registered in the neighbouring country and used for travel between Slovenia and that country. The Police requested and obtained additional information from the neighbouring counterparts, based on a bilateral police cross-border cooperation agreement. Following this exchange, the prosecutors from that country requested access to the information held by the Slovenian prosecution service through an EIO. Slovenian prosecutors cooperated effectively with their counterparts, providing relevant information and evidence. The information enabled the foreign authorities to initiate criminal proceedings against three individuals suspected of drug trafficking, committed as part of an organised criminal group.

170. Judicial authorities also collaborate with their foreign EU counterparts to address various issues, including jurisdictional conflicts, problems arising from requests of insufficient quality, identifying comparable measures under national law, and requesting additional explanations or information. Cooperation with European Judicial Network (EJN) contact points and Eurojust facilitates solution finding. Based on the received feedback, the authorities demonstrated willingness to provide guidance to prevent misunderstandings and delays in responses to EIOs.

171. While the lack of comprehensive statistics for this type of cooperation does not have direct impact on the quality and timeliness of the assistance provided, it does limit the country's ability to fully monitor whether it is effectively providing and seeking international cooperation and prevents them from developing a full overview of crime trends.

2.1.2 Extradition

172. Slovenia receives on average 60 requests for extradition per year, most of which are coming from EU Member State as EAWs.

173. The authorities, similar as for the MLA requests, presented statistics on the number of extradition requests per predicate offences concerning those originating from non-EU member states. Based on the data, it can be concluded that majority of requests related to the predicate offences posing ML threat and refusal rate is reasonable. The AT identified that 9 requests (≈13%) were refused on the following grounds: (i) violation of Art. 3 of the ECHR; (ii) violation of the *ne bis in idem* principle; (iii) the person sought was not in Slovenia; (iv) statute of limitation or (v) the person sought was a Slovenian national. The authorities are commended for the gradual improvement of the average execution time of the extradition requests from 174 days in 2020 to 80 days in 2024.

174. Feedback from the global network indicate extradition requests were successfully executed by Slovenian authorities.

175. Slovenian MoJ provides feedback to foreign countries requesting extradition, for example in cases where there are concerns with respect to the fairness of proceedings.

Table 2.3. Incoming extradition requests (from non-EU countries)

Incoming extradition requests (non-EU)	2020	2021	2022	2023	2024	TOTAL
ML	2					**2**
TF	2					**2**
Drug trafficking	**7**	**3**	**1**	**3**	**5**	**19**
Participation in an OCG and racketeering	**2**		**1**			**3**
Trafficking in human beings and migrant smuggling	**1**	**1**	**3**		**1**	**6**
Sexual exploitation, including of children			**2**			**2**
Illicit arms trafficking					**1**	**1**
Corruption and bribery	**2**	**1**	**1**			**4**
Fraud	**6**	**4**		**3**	**2**	**15**
Murder, grievous bodily injury					**1**	**1**
Kidnapping, illegal restraint and hostage-taking		**1**				**1**
Robbery or theft	**2**	**2**	**1**	**2**	**2**	**9**
Smuggling (including in relation to customs and excise duties and taxes)	**1**					**1**
Tax crimes (related to direct and indirect taxes)	**1**					**1**
Extortion	**1**				**1**	**2**
TOTAL	**27**	**12**	**9**	**8**	**13**	**69**

Source: MoJ

176. As stated above, the majority of requests for extradition are coming from EU Member States. The authorities were not able to provide statistics on the number of EAWs per predicate offences. Nevertheless, the AT was able to draw several conclusions:

177. Except for 2024 – for which limited data is available, in almost 90% of the cases, the sought persons were arrested, while in 67% of the cases the persons were effectively surrendered. Slovenia refused to execute 21 EAWs (≈ 8.8%) based on (i)violation of the *ne bis in idem* rule, (ii) territoriality overlap, (iii) statute of limitation or (iv) the persons being Slovenian nationals. In almost all cases, Slovenia respected the 90-day time limit for the decision on the execution of EAWs.

178. In cases where Slovenia refuses to extradite criminals because they are Slovenian nationals, the case files are handed over to prosecutors for them to explore if there are grounds to initiate domestic criminal proceedings. MoJ advised that in the evaluated period they had one successful case of prosecution of a Slovenian citizen whose extradition was refused. State Prosecutor's Office advised that where the Criminal Code (CC) provisions on territorial applicability allow its application, the prosecution of a Slovenian national committing crimes abroad is required (under the same conditions as in domestic cases) if sufficient evidence exists to establish reasonable suspicion that crime has been committed. However, in practice, prosecution in Slovenia starts only if the country requesting extradition requests the commencement of prosecution in Slovenia, as prescribed by international agreements (e.g. Art. 6/II of the COE Convention on extradition).

Table 2.4. Incoming EAW

Incoming European Arrest Warrants	2020	2021	2022	2023	2024
Received EAW	44	61	77	57	91
Arrested persons	39	51	73	51	N/A
Effectively surrendered persons	**29**	**36**	**60**	**36**	N/A
Refused	**3**	**6**	**7**	**5**	N/A
Average execution time for the persons who consented the surrender (days)	**4.5**	**7.8**	**18**	**17.6**	N/A

2.1.3 Facilitate asset recovery

179. In Slovenia, the authorities execute requests concerning seizure of assets on behalf of other countries, irrespective of whether they are EU or non-EU member states. These requests are generally received as European freezing orders (EFOs) or through MLA requests if they originate from non-EU Member States.

180. Requests for seizing, freezing and confiscation of assets are referred to the competent courts for execution, as coercive measures fall within their jurisdiction.

181. The fact that there are no exact figures on the number of requests received from foreign countries for the freezing, seizure, confiscation, and sharing of criminal assets raises concerns over the authorities' ability to properly analyse the level of criminality in the country and potentially apply some measures to mitigate the issue. However, when it comes to the execution of foreign requests, the authorities demonstrated the effectiveness and the commitment to act swiftly and decisively (see box 2.4). This is also supported by the feedback received from the global community which shows that Slovenia provided good quality and smooth cooperation, traced and identified assets, with no delays in responses.

Case Box 2.4: Freezing of assets

On 7 October 2024, the District Court of Ljubljana received an urgent request from an Austrian Court to temporarily freeze assets under Regulation (EU) 2018/1805. The request pertained to a case involving fraudulent misuse of data processing and money laundering, with Slovenian authorities asked to freeze assets totalling EUR 61 750 held in the bank accounts of two Slovenian individuals. The court granted the request on 11 October 2024, ensuring the assets were successfully frozen without delay, demonstrating efficient cross-border cooperation.

Source: Supreme court

182. The ARO contact prosecutor, established within the Supreme State Prosecutor's Office, has access to SIENA communication platform since 2023 - where it exchanges information directly with other EU countries. This in practice facilitates the identification and seizure of assets when requested from foreign counterparts.

183. In order to facilitate asset recovery, when requested, prosecutors provide banking information. Slovenian prosecutors presented several EIOs and MLA requests for which they provided different types of evidence such as banking information to foreign counterparts, facilitating thus the identification and tracing of criminal assets.

2.2. Seeking appropriate and timely mutual legal assistance and extradition

2.2.1. Seeking evidence and locating criminals

184. Slovenian judicial authorities proactively seek assistance from foreign countries, including from EU and non-EU member states. The AT formed a conclusion on the effectiveness of this type of international cooperation based on the available data, interviews held onsite, international feedback, and a number of cases presented by different competent authorities. Feedback received from the global network reveals that Slovenia's MLA requests meet the quality and the parameters required by international legal instruments. Also, it can be concluded that Slovenia seeks MLA from countries all over the world (e.g. Hong Kong), as well as from Western Balkans and Switzerland, but most often from EU countries, specifically from Germany, Italy, Malta, Poland or Latvia, in which instances they use EIOs. This is broadly in line with country's risk profile.

185. As explained under the previous core issue, only MoJ is able to provide statistics on the number of MLA requests sent for ML, TF and predicate offences. It can be concluded that the authorities actively and strategically seek international assistance from non-EU member states in both ML and predicate offences cases. During the assessed period, 61 outgoing MLA requests representing 3.8% of all outgoing requests were specifically related to ML offences.

186. When pursuing predicate offences, for instance, 34% of outgoing MLA requests relate to fraud, 34.5% to migrant smuggling, approximately 8% to drug trafficking, and 6.7% to sexual exploitation—reflecting the primary areas of ML risk identified for Slovenia.

Table 2.5. Outgoing MLA requests

Outgoing MLA	2020	2021	2022	2023	2024	TOTAL
ML	11	16	11	15	8	**61**
TF	-	-	-	-	-	**0**
Drug trafficking	22	15	24	37	28	**126**
Participation in an organised criminal group and racketeering	1	1	3	1	3	**9**
Trafficking in human beings and migrant smuggling	68	74	95	125	187	**549**
Sexual exploitation, including of children	19	19	20	29	21	**108**
Illicit arms trafficking	5	2	3	4	5	**19**
Corruption and bribery	1	5	2	3	1	**12**
Fraud	103	122	141	95	81	**542**
Counterfeiting currency	1		1	3	5	**10**
Murder, grievous bodily injury	2	6	3	3	5	**19**
Kidnapping, illegal restraint and hostage-taking		-	7	2	2	**11**
Robbery or theft	13	11	12	6	16	**58**
Smuggling (including in relation to customs and excise duties and taxes)	1	3	1	1	3	**9**
Tax crimes (related to direct and indirect taxes)	2	-	-	-	-	**2**
Extortion	6	4	7	12	6	**35**
Forgery	5	4	2	2		**13**
TOTAL	**262**	**284**	**333**	**341**	**371**	**1591**

187. The figures per crimes for EIOs are not available and the AT used interviews and case examples to establish the extent to which the assistance is sought proactively and in line with country's risk profile.

Given that cooperation with EU is conducted in a decentralised manner, the Slovenian courts and prosecutors have separately provided statistics on the number of EIOs issued during 2020-2025. For example, courts issue on average 585 per year while prosecutors – on average 220 per year. A notable increase was observed in 2024 and 2025, with EIOs issued in 636 and 714 cases, respectively. This rise is attributed to the increase in fraud-related cases which also corelated with the risk trend in the country. Thus, in practice, the increase of the evidentiary threshold has not impacted on the level of assistance sought.

188. There are a number of case examples presented by the authorities, demonstrating that they proactively seek international cooperation from other EU Member States. Some statistics are available for the EIOs sent through the EUROJUST. Based on that, the most frequent offences, for which EIOs were sent, were: fraud (including business fraud), tax crimes, drug trafficking, arms trafficking, ML - which is largely in line with the risks identified under the NRA.

189. There were no outgoing MLA requests or EIOs related to TF between 2020-2024, which is also in line with the low TF risk in the country.

Case Box 2.5: Gathering evidence abroad through EIO

Case example 1 In 2022, a Slovenian court obtained banking information through an MLA request. The information was used to file an indictment with a request for the issuance of a penal order against a foreign national for aiding and abetting the commission of fraud. The judgement has become final.

Case example 2 In 2021, in a case handled by SPO, related to drug trafficking, an EIO was submitted to the competent foreign authorities by email. Slovenian authorities sought obtaining SKY ECC evidence, which was already possessed by the authorities of the requested state. A response was received in the same day.

190. The most common requested measures related to information on previous criminal offences, convictions, banking data, telecommunications traffic data, data from official registers witness and suspect hearing, etc.

191. Slovenian authorities actively participate in JITs which are formed based on their initiative or are created by other countries. The authorities have presented a number of cases where JITs were established in order to dismantle complex ML, tax evasion or organised crime cases (See case box 7.1). Similarly in one case the SPO investigated, within the framework of a JIT, a large financial crime network in the region involving 64 suspects and multiple offences.

192. Overall, the statistical data and contextual information confirm that Slovenia is proactive and methodical in seeking assistance from foreign counterparts for both ML and predicate offence cases. By utilizing the full range of available legal instruments, Slovenian authorities effectively support the investigation and prosecution of cross-border financial crime in accordance with international standards.

2.2.2 Extradition

193. Slovenian authorities regularly ask for assistance from foreign countries to seeking criminals. Most of the extradition requests are directed to EU Member States using EAWs.

194. During 2020-2024, authorities mainly sought from non-EU jurisdictions extradition of offenders implicated in fraud, theft, human trafficking, drug trafficking, sexual exploitation, murder, counterfeiting currency and tax-crimes (See table 2.6). Some of these requests were addressed to Balkan countries, which is broadly in line with the country's risk and context. Around 17.5% of all requests were refused on grounds

of lack of dual criminality, the statute of limitations, or because the person sought was a national of the requested state.

Table 2.6. Outgoing extradition requests

Outgoing extradition requests	2020	2021	2022	2023	2024
ML	1	0	0	0	1
TF		0	0	0	
Drug trafficking	1	1		1	1
Trafficking in human beings and migrant smuggling	0	0	2	0	3
Sexual exploitation, including of children	1	0	2	0	1
Fraud	4	3	3	1	1
Counterfeiting currency	1	0	0	0	
Murder, grievous bodily injury	0	0	0	1	1
Robbery or theft	1	2	0	3	0
Tax crimes	1	0	0	0	0

195. During the 2020-2024, Slovenia issued 413 EAWs to EU-states. More than half of them were issued for the purpose of prosecution. The most common categories of predicate offences underlying the issuance of EAWs were fraud and corruption, theft, drug-related offences, sexual offences, counterfeiting of the euro, and other offences. No EAWs were issued in relation to terrorism or terrorist financing, which is consistent with the country's risk profile. However, there is a lack of comprehensive statistics for EAW (see table 2.7).

Table 2.7. Outgoing EAW

Outgoing European Arrest Warrants	2020	2021	2022	2023	2024
EAW Sent	**90**	**93**	**85**	**70**	**97**
EAW issued for the purpose of prosecution	56	62	49	40	N/A
Effectively surrendered persons	**21**	**24**	**42**	N/A	N/A
Refused	N/A	N/A	N/A	N/A	N/A

Case Box 2.6: Successful extradition to Slovenia

A Slovenian fugitive was hiding in overseas Country X. The Slovenian MoJ sent the extradition request and documentation to the central authority of Country X for the purposes of execution of sentences and conducting criminal proceedings for the offences of robbery, fraud, and concealment. The requested authorities granted the extradition of the person in 2021. The surrender of the fugitive to Slovenian authorities took place during the Covid lockdown, at a time when they were flight disruptions. To facilitate the transfer, the authorities arranged a private jet to fly directly to Country X to retrieve the suspect.

This example demonstrates the successful results achieved through close and effective cooperation between the Slovenian and authorities of Country X, despite the challenging circumstances.

2.2.3 Seeking to facilitate asset recovery

196. Slovenian authorities lack statistics regarding requests for mutual legal assistance relating to asset recovery matters. However, the competent authorities have provided some good case examples where their freezing orders were recognised and executed in foreign countries. Mostly, these freezing and confiscation orders were related to fraud offences, ML and abuse of position or trust in business activity, which is largely in line with the risk profile of the country. As an example, in 3 cases from 2020-2024, two neighbouring countries successfully froze funds totalling approx. EUR 285 000 at the request of Slovenian authorities.

197. A case where Slovenia cooperated with another EU country based on Warsaw Convention was presented to the AT as it led to the first asset-sharing agreement concluded in Slovenia. Initiated by Luxembourg and following coordination with Slovenia, the parties agreed to equally share crypto assets confiscated in Luxembourg, which were already converted to Euro.

198. However, there are some challenges in seeking property moved abroad. Namely, the high evidentiary threshold established by courts require authorities to demonstrate that assets are still available in the foreign accounts in order to acquire court order necessary to further request seizing these assets aboard. This seems to be particularly significant in the context of cybercrime, where authorities are required to act swiftly to prevent the dissipation of the crime proceeds.

2.3. Seeking other forms of international cooperation for AML/CFT purposes, including asset recovery

2.3.1 FIU

199. The OMLP is committed to international cooperation, proactively requesting information from foreign FIUs through dedicated secure channels (ESW and FIU.net) when more information is needed to enhance their operational analysis in cross-border cases. The OMLP has the good practice of submitting feedback to its international counterparts. The quality and clarity of its requests have been recognised by the global network. Within the OMLP, a dedicated analyst handles the requests received from foreign counterparts. Besides, an international cooperation department is established within the FIU, supporting also the needs of the Suspicious Transactions Sector (operational analysis department).

200. In general, the number of outgoing requests is higher than the number of the incoming ones. Over the last 6 years, except for 2022, a significant increase in the number of requests transmitted by OMLP has been observed. This is due to the increase of ML cases stemming from fraud. The number of outgoing TF requests is low (19), which is in line with Slovenia's low risk for TF. In none of the instances was an OMLP request refused, which is an indicator of the good quality of the outgoing requests and of OMLP's engagement in international cooperation. The counterparts from which the OMLP most frequently requests information are the FIU of Germany and Italy, which is broadly in line with the country's risk and context, given Slovenia's strong economic and social ties with these countries.

Table 2.8. OMLP outgoing requests

OMLP outgoing requests	2020	2021	2022	2023	2024	First half of 2025
ML	344	354	257	467	583	230
TF	1	0	0	3	8	7

201. Although no statistics were provided on the number of requests sent by OMLP to foreign FIUs regarding freezing of funds, cases show that OMLP regularly seeks suspension of transactions. The authorities advised that the number of such requests increased significantly in the last years, as a result of

an increasing trend in fraud cases, which almost always have an international element.

2.3.2 Law enforcement agencies (LEAs)

202. The Police request information related to ML, associate predicate offences from foreign counterparts for both intelligence and pre-investigative purposes. Slovenian Police make use of its powers to cooperate both within and outside EU also through Europol-SIENA, Schengen Information System and Interpol I-24/7 dedicated channels. The police have developed internal guidance regarding international exchange of information as a tool to assist investigators in criminal investigations, which is accessible to all criminal investigators nationwide. A practical guide covering multiple countries is also available to police officers, providing clear, concise information on what data can be obtained from each country, the type of request required, expected timeframes, and the relevant foreign contact points. Also, internal guidelines on international cooperation matters are published on their intranet, covering areas such as extradition, cross-border covert surveillance, access to different databases, etc.

203. Slovenian Police officers from different units (Economic Crime Unit, National Bureau of Investigation and Regional units) demonstrate a high level of commitment for international cooperation, making regular and effective use of the available communication channels in the course of their operational activities to investigate criminal offences. For example, in the case described under IO.7 (see Box case 7.1), police used extensive cooperation mechanisms, including EUROPOL, which helped them identify suspects and start the investigation.

204. Additionally, Slovenian Police successfully request information based on bilateral and multilateral agreements, making efficient use of the available Europol and Interpol communication channels. Several fraud and ML cases with funds of significant value were presented, showcasing the ability of the Slovenian Police to identify, trace, freeze and recover fraudulent funds in EU and non-EU jurisdictions.

205. Under the coordination of state prosecutors, the Police participated in 2 JITs set by Slovenia, where cooperation was carried out swiftly between different national and foreign law enforcement authorities. This type of cooperation is appreciated by the Slovenian LEAs, as it allowed direct exchange of evidence between investigators from different countries.

206. During 2020 and the first half of 2025, the Police has sent 1945 ML requests (including additional requests) to foreign LEAs and 4 TF requests. The countries to which requests were most frequently forwarded via the Interpol channel were the United Kingdom, Ukraine, Russia, Serbia, and Switzerland, while requests submitted through Europol Siena were mostly forwarded to Germany, Italy, Croatia and Austria, which is largely in line the country’s transnational risk.

207. Slovenian prosecutors engage in informal cooperation with foreign counterpart via the Police given that investigation is conducted by the investigative judges. In urgent cases, direct contact and established professional networks are commonly used by prosecutors to coordinate with foreign authorities in advance on matters regarding the form and content of MLA requests, ensuring their timely and effective execution.

2.3.3 Supervisors of FIs, VASPs and DNFBPs

208. The BoS regularly exchanges information with foreign supervisors, those of subsidiaries and branches located in Slovenia and Slovenian banks’ branches located abroad. Among other, the information relates to emerging risks, trends identified, licensing and relevant findings of inspections. Additionally, the BoS exchanges information in the framework of EBA and ECB supervisory colleges. In 2020 and 2024 BoS organised and hosted AML/CFT Supervisory Colleges, which served as a platform for cross-border information exchange and coordination among supervisory authorities overseeing FIs operating in the

region.

Table 2.9. BoS - Outgoing requests

Outgoing requests	2022	2023	2024	First half of 2025
- Fit and proper, qualifying holding and extension of license procedures	19	22	13	4
- Supervision and sanctions	0	1	6	0
Total	**19**	**23**	**19**	**4**

209. In the fit and proper assessments conducted by BoS, many candidates have work experience solely within Slovenia, making inquiries to foreign supervisors unnecessary. For candidates with prior experience in entities supervised exclusively by the ECB, BoS requests complete suitability information only from the ECB, regardless of the MS where the institution is registered.

210. Additionally, as other EU financial supervisors, BoS has access to EuReCa database (managed by EBA), where it enters data on significant AML/CFT weaknesses identified during its supervision activities at FIs - together with the corrective measures/sanctions imposed. This kind of information is then directly available to BoS and other EU supervisors, removing the need for formal requests between authorities.

211. SMA seeks international assistance based on IOSCO and ESMA multilateral cooperation agreements. Obliged entities under SMA's remit are mainly domestic entities, with insignificant international business scale.

212. ISA has legal powers to cooperate with foreign supervisory authorities. In 2020 and 2024 ISA sought assistance from a regional non-EU counterpart to obtain fit and proper information on a candidate for the Management Board of a Slovenian insurance company, with respect to licensing of specialised fund manager and alternative investment fund. The received information supported ISA's decision.

213. Licensing and supervisory authorities for DNFBPs have little exposure to international cooperation due to predominantly domestic nature of the sectors covered.

2.3.4 Custom and tax authorities

214. In Slovenia, the FARS is the national tax and customs authority. It actively exchanges VAT information with other EU Member States, data on direct taxes, and customs with both EU and non-EU countries (see table 2.10). Since 2023, the volume of outgoing exchanges has almost tripled, which underlines the engagement of FARS in international cooperation.

215. FARS is well resourced, having a dedicated international cooperation unit established with 12 staff members dealing exclusively with international requests, and another unit of 10 staff members dealing with exchanges. Requests for information in the area of tax, excise duties and customs are received and sent daily to international counterparts. Most of the requests concern VAT issues and are sent within EU, Austria being one of the main recipients of their requests.

216. At the request of foreign counterparts, FARS initiates financial investigations according to the Tax Procedure Act. When international requests are received, FARS collects data from the tax database and other databases and performs a risk analysis and initiates tax audits in case risks are identified.

Table 2.10. FARS – Outgoing requests and exchanges

Outgoing exchanges and requests in the field of:	2020	2021	2022	2023	2024	First half of 2025
VAT	465	651	295	391	428	266
Direct taxes	351	221	310	917*	950*	551*
Customs	50	19	16	39	43	25

* The data for 2023 -2025 deviates due to an increase in Requests for notification and Bulk service documents sent to Austria.

217. FARS presented a case that captures good cooperation with regional non-EU counterparts: a national of a Western Balkan country suspected of ML attempted to smuggle undeclared cash into Slovenia for subsequent transfer to another EU country. Based on a bilateral agreement, FARS requested and successfully obtained data on the suspect's employment, bank accounts, registered business activity from the authorities of his country of origin.

218. According to the feedback from the international network, FARS often seeks assistance from foreign customs authorities, especially from Germany and neighbouring countries, which is in line with the country's risk and context, particularly given its strong economic ties with neighbouring EU countries and its role as a transit country along the Balkan route towards the EU and the Schengen Area.

2.4. Providing other forms international cooperation for AML/CFT purposes, including asset recovery

2.4.1 FIU

219. OMLP is committed to promoting effective and high-quality international cooperation by ensuring that information and assistance are provided in a timely and efficient manner. Financial intelligence or information shared by OMLP, both spontaneously and upon request, is appreciated by its foreign counterparts. The availability of an adequate number of databases to which the FIU has access (see IO.6), including RBO, contributes significantly to the quality of its responses. Nevertheless, the shortcomings identified under IO.5 regarding the accuracy of BO information may limit the quality and reliability of the assistance provided by OMLP to its foreign counterparts. Nevertheless, no negative feedback on Slovenia's ability to provide BO information was signalled by the global community.

220. At the request of a foreign counterpart, OMLP withholds suspicious transactions for 3 business days, facilitating thus the asset recovery process.

221. The volume of requests received by OMLP (562) in the last 6 years is significantly smaller than the volume of the ones sent. A decreasing trend was observed over the years in the incoming requests. Between 2020 and the first half of 2025, the OMLP responded to almost all the foreign requests (with one exception from 2025), in an average time of 24 days, which is reasonable. Spontaneous disseminations were regularly submitted to foreign FIUs when links to their jurisdictions were discovered during OMLP's analyses.

Table 2.11. OMLP - Incoming requests

OMLP incoming requests	2020	2021	2022	2023	2024	First half of 2025
ML	139	134	99	84	69	33
TF	2	7	8	6	6	1
Total	**141**	**141**	**107**	**74**	**65**	**34**

Pending						**1 (ML)**
Average response time (days)	**23**	**35**	**10**	**23**	**29**	**23**

Source: OMLP

222. In March 2025, OMLP sent a survey to 20 FIUs with which it most frequently exchanges information to evaluate the quality and timeliness of its assistance. The results indicated that 90% of respondents were highly satisfied with the promptness and usefulness of OMLP's responses, and all confirmed that OMLP had addressed all their questions.

2.4.2 Law enforcement agencies (LEAs)

223. Slovenia's LEAs maintain frequent and effective informal international co-operation with foreign counterparts from EU and non-EU Member States, including through Europol and Interpol. Within the Slovenian Central Police Department, a special unit dealing with international cooperation is established, acting as a single 24/7 contact point for international requests, monitoring the execution of requests through a case management system. Incoming requests are promptly assigned to the relevant regional or local police units with the indication of the deadline for the response. The responses sent are generally complete, making use of the date from the available databases, and are provided in a timely manner. Between 2020 and the first half of 2025, the Police indicated that it received 2 548 ML requests (including additional requests and replies) from foreign LEAs and 14 requests related to TF. International cooperation feedback indicates that fraud, ML, robbery, constitution of criminal organisations and computer crimes are the most frequent offences they request assistance from Slovenia.

224. Prosecutors mainly provide information to foreign LEAs through MLA/EIO requests. They frequently initiate and take part in JITs, when necessary, involving the Police.

225. Slovenia regularly provides assistance related to asset recovery through the Slovenian ARO contact point – the prosecutor at the Supreme State Prosecutor's Office, which has access to EUROPOL SIENA since 2023. It exchanges requests directly with other AROs of EU Member States. Foreign requests received by the ARO contact point are forwarded to the Criminal Police Directorate and to the OMLP for collecting necessary information. Once the requested information is gathered, a response is forwarded by the Slovenian ARO contact point to the requesting ARO.

2.4.3 Supervisors of FIs, VASPs and DNFBPs

226. BoS provides assistance to foreign supervisors on a regular basis. The number of incoming requests has slightly increased over the period under review. The below statistics capture the engagement of BoS to provide assistance to all requests received in a prompt manner. The AT observes improvements in the response time of BoS in 2025, compared to the previous years.

Table 2.12. BoS – Incoming requests

Incoming requests	2020	2021	2022	2023	2024	First half of 2025
- Fit and proper measures	6	5	9	9	8	3
- Supervision and sanctions	1	2	2	1	1	0
Total	7	7	11	10	9	3
Requests responded:						
- Fit and proper measures	6	5	9	9	8	3

- Supervision and sanctions	1	2	2	1	1	
Total	7	7	11	10	9	3
Requests pending	0	0	0	0	0	0
Requests refused	0	0	0	0	0	0
Average response time (days)	17	15	17	13	16	10

227. BoS presented examples of provided cooperation (upon request and spontaneously) to foreign NCAs relating to VASPs, demonstrating their ability to cooperate timely and effectively. Additionally, as mentioned under the previous section of this chapter, BoS informs EBA on the findings of its supervision activities through EuReCa (EBA's AML/CFT database).

228. ISA did not provide statistics on the incoming requests related to fit and proper assessments, sanctions imposed or group supervision of obliged entities under its remit. Feedback from the international counterparts revealed, however, that in 2023 they promptly and successfully provided assistance to a regional non-EU counterpart on the suitability and reputation of several Slovenian insurance undertakings.

229. In respect to the medium-low risk profile of its supervised entities, SMA has sufficient resources to promptly exchange information with foreign supervisory authorities. An international cooperation section is established within SMA, consisting of two employees, responsible for international cooperation. In the period under review, eight requests have been received, all of them related to fit and proper checks, supervision and sanctions. Only one request regarding supervision and sanctions was refused. SMA advised that such refusals occur when the request is outside the scope of its competence or when it originates from third countries that have not signed a multilateral arrangement for the exchange of personal data.

2.4.4 Customs and tax authorities

230. FARS is efficiently cooperating and is engaged in daily exchanges with foreign counterparts, on AML/CFT matters, providing information on VAT, direct taxes, and customs both at request and in the framework of automatic exchanges. Most international exchanges take place with Slovenia's neighbouring countries: Austria, Croatia, Italy which is in line with the country's risk profile. FARS provided the statistics for the number of incoming requests regarding VAT, direct taxes and customs information for the period 2020 to the first half of 2025. Namely, 2 063 requests related to VAT, 522 – to direct taxes, and 512 to customs. When requests relate to AML/CFT, they are prioritised and handled in a more expedited way.

231. Some foreign counterparts consider the information provided by FARS to be useful, smooth and reliable, allowing them to initiate customs enforcement procedures and strengthen control measures. The most frequent requested information relates to the verification of invoices authenticity, cigarette smuggling or other excisable goods, and drug smuggling.

Chapter 3. Financial Sector and Virtual Asset Supervision and Preventive Measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.3.[18] *The Recommendations relevant for the assessment of effectiveness under this chapter are R.9-21, 26, 27, 34 and 35 and elements of R.1, 29 and 40.*

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) The Authorities' ability to limit the presence of criminals and their associates within the ownership and control structure of FIs is overall good. The regulatory framework for VASPs is now aligned with that of material FIs. Authorities for the more material sectors have demonstrated an ability to filter through authorisation applications which were dubious, including the ones for the VASPs. Authorities take a reactive approach to identify situations where one is no longer fit and proper, though they are more proactive when it comes to identifying the carrying out of unauthorised activities.

b) Authorities have not carried out specific sectoral risk assessments but their role within the NRA process shows that they have an effective understanding of the risks presented by the FIs and VASPs under their respective remit. All the main AML/CFT supervisors have a risk assessment process in place for their OEs, though the depth of these varies, at times even between sectors. While supervisory judgement still plays a role within the risk assessment process, the possible subjectivity that may result therefrom is mitigated through the application of the four-eye principle.

c) All FIs and VASPs agreed with the analyses of their respective sectors in the NRA and the results of the analyses, with especially key institutions being able to describe not only the main ML/TF risks they are exposed to but how they may materialise and how they can be effectively mitigated.

d) All authorities are accessible to OEs to discuss questions and issues that may arise in the implementation of AML/CFT obligations, and all have provided their supervised OEs with guidance documents and trainings. This may account for the good grasp that the obliged entities have of their obligations shown during the on-site.

e) Authorities have, to different degrees, undertaken supervisory examinations on the OEs falling within their remit. The number of full-scope examinations is not significant, but this is reflective of the overall ML/TF risk of the different sectors and OEs. In addition, a number of thematic reviews have been carried out by the different authorities, some of which take into consideration quite a number of AML/CFT obligations so as to be quasi full-scope ones. Resource limitations hamper the development and implementation of supervisory plans. Though efforts are being made to ensure more effective information sharing on supervisory plans, coordination of supervisory activities is limited.

18. When assessing effectiveness under Immediate Outcomes 3, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of Financial Institutions and VASPs, as required in the instructions under that heading in the Methodology.

f) Authorities apply a wide range of supervisory measures to ensure the remediation of identified issues. Overall, all authorities take follow-up measures to ensure the correct implementation of the necessary changes, with the BoS also carrying out follow-up examinations. Where remedial action is not taken on time, additional supervisory measures and enforcement actions, including the imposition of pecuniary fines, are applied.

g) The BoS has also taken a series of enforcement actions on FIs and their responsible officers, resulting in both pecuniary fines and reprimands. However, the need to carry out misdemeanour procedure to impose fines presents a limitation on the ability of the supervisory authorities to ensure the proportionality of its sanctioning measures due to the possible reduction of any fine imposed by half and the application of prescription. Misdemeanour procedures also result in the imposition of sanctioning measures on individual officers though these may not necessarily be proportionate to the seriousness of the identified breaches.

Key Recommended Actions (KRA)

N/A

Other Recommended Actions

a) Slovenia should continue enhancing effectiveness of the risk-based supervision across FI and VASP sectors including by improving the planning of frequency and intrusiveness of supervisory activities and making a wider use of its different supervisory tools. Slovenia should increase supervisory capacities and cooperation, as well as human resources at all supervisors.

b) Slovenia should continue strengthening its efforts in imposing proportionate, effective and dissuasive sanctions and ensure that any limitations resulting from the misdemeanour procedure are addressed.

c) All licensing authorities should refine their procedures and strengthen their controls to enable applying more proactive measures so that market entry requirements are met on an ongoing bases for FIs and VASPs.

d) All supervisory authorities should strengthen the methodologies used for OE level and sectoral risk assessments to ensure that their risk understanding is always up-to-date.

Overall Conclusions on IO.3

Slovenia has significantly robust market entry requirements for material FIs, with minor issues identified in terms of ensuring that these are met on an on-going basis. Market entry requirements for VASPs were much lighter for most of the evaluation period. These have now been aligned with those applicable to FIs but more attention should be paid to detecting unauthorised VASPs.

Authorities' supervisory activities are proving to be effective as demonstrated by both the outcome of supervisory actions as well as from the meetings had with OEs. The main supervisory tool is the thematic examination, which at times does cover quite a wide range of obligations as to be a quasi-full-scope examination. This is also reflective of the overall risk of the different sectors and OEs under consideration. Supervisory activities are impacted by a lack of resources on the part of all authorities.

In the event of findings, authorities are taking a number of informal and formal remedial actions, depending on the severity of the findings. Authorities' actions when it comes to enforcement are being impacted by some provisions of the misdemeanour procedure, at times limiting the proportionate, effective and dissuasive nature of the enforcement actions they take.

Slovenia is rated as having a substantial level of effectiveness under IO3.

232. The AT applied the following weighting to assess the implementation of preventive measures by FIs and VASPs: extremely important for banks; very important for EMIs, PIs and VASPs; moderately important for investment service providers, collective investments schemes; and less important for the insurance sector other FIs.

3.1. Licensing, registration and controls for FIs and VASPs preventing criminals and associates from entering the market

BoS

233. The BoS is licensing banks, EMIs, PSPs and foreign currency exchange offices. The same process is applied to authorise any such entity and approve individuals involved with the same (inc. qualifying shareholders and their BOs, members of the supervisory and management bodies). The main source of information with any application is the information and documents provided by the applicant itself, including a questionnaire completed by anyone that has been designated to sit on the management or supervisory board of the same, anyone that has to acquire a qualifying shareholding, and, where applicable, the shareholder's BOs. The questionnaire is used to collect information on the education, professional experience and qualification, financial standing and character of the individual, including possible investigations, prosecutions and convictions the applicant is aware of. In all instances, supporting documents have to be provided, including an official record of the individual's criminal conduct. In the case of qualifying shareholdings, information has also to be provided with regards to the source of funds to be used for the acquisition of the shareholding.

234. The BoS supplements the information and documents provided by the applicant through its own checks. These checks include open-source intelligence (OSINT), sanction lists and information from its domestic counterparts where the entity may already be licensed by another authority or the individual sets out in the questionnaire that it had been previously approved by another authority. Each application also triggers checks with the OMLP. The BoS also seeks information from the Police and the Prosecutors. These checks can be of significant importance to mitigate the chance of criminal associates infiltrating authorised entities.

235. In processing applications, the BoS seeks to make the widest possible use of information from its foreign counterparts. Examples were provided where the BoS sought information on entities and individuals that were seeking authorisation to acquire qualifying shareholdings and appointment to the management board respectively, including requests to supranational authorities like the ECB.

Box 3.1. BoS - Acquisition of a qualifying shareholding

In 2022, a legal person sought to acquire a qualifying shareholding in a Slovenian bank. As part of its application process, the BoS requested information from a number of sources including the OMLP. On the basis of the intelligence obtained, the BoS was intent on refusing the application but in this case the actual authorisation had to be obtained at the supranational level, with the ECB considering that the information did not justify a refusal. A decision was taken to grant a conditional approval subject to regular reporting on how the applicant was meeting the conditions imposed by the ECB.

236. The BoS has also demonstrated its ability to analyse and identify potential issues with licensing applications when it comes to entities other than banks. In one case it rejected an application for an EMI authorisation on the basis that there were concerns about the reputation of the members of the management and supervisory board and also in relation to whether the BO of one of the qualifying shareholders was the actual owner or a strawman. The checks applied by the BoS are therefore considered sufficiently robust to identify possible criminal infiltrations, including through associates, into the FIs falling within its remit.

237. Over the years, there have been a series of withdrawal of applications. In such cases, the BoS still retains a record of these applications which can be made available to other authorities upon request.

238. As regards ensuring that licence-holders and/or individuals involved with the same remain fit and proper, the BoS relies on a series of triggering events, including information provided by the OE itself or the involved individuals, information obtained through supervisory activities and other information received from the public or other authorities, be they local or foreign, including supervisory colleges in the case of FIs having cross-border activities.

239. On the other hand, the BoS actively monitors a series of sources to ensure that no unauthorised activities are being carried out. These include checks related to requests to access the central credit register, whistleblowing reports and reports from foreign counterparts. By way of example, the BoS has carried out at least three (3) in-depth analyses on entities that were allegedly carrying out banking business. None of these resulted in any action as in two (2) cases the concerns were discarded whereas in one (1) case directions were given to stop unintentionally accepting deposits. On the other hand, two companies were placed into liquidation in 2019 due to their accepting deposits from the public without the necessary banking authorisation.

240. As to the possibility that the BO changes, someone acquires a qualifying shareholding or is appointed to the supervisory or management body without the BoS consent, the authorities advised that no such instances have been encountered so far. In the case of changes to the management or supervisory body, the registration of a change through the Court Register would require presenting the BoS' approval for the said appointment. In the other cases, there is no similar limitation to the registration of a change in either BO or shareholder, other than the FI's own obligation. The FI could very well proceed with the registration without the necessary checks having been carried out by the BoS, weakening the ability of authorities to limit criminal infiltration in the management of FIs.

SMA

241. The SMA is licensing investment service providers and investment management companies for collective investment schemes. Collective investment schemes are also subject to licensing by the SMA but checks are focused on conduct of business and prudential requirements. Given the particular form that collective investment schemes take, i.e. either as contractual funds or as limited partnerships, the main party thereto would be the already licensed investment manager and therefore no additional checks would be

necessary. The licensing process applied to investment service providers and investment management companies is quite similar, the main element consisting in the submission of a licence applications with relevant documents and the submission of a questionnaire for anyone designated to hold a qualifying shareholding and, where applicable, its BOs, or to sit on the management or supervisory board. In the case of the qualifying shareholder, there would also be checks carried out on the source of the funds to be used to acquire the said shareholding.

242. The authorisation of qualifying shareholders, its BOs (where applicable), and of members of the management or supervisory board heavily depends on the information OEs provide in their respective questionnaire as to whether they or, in the case of qualifying shareholders, their BOs have been subject to investigation, prosecution or conviction for specific criminal offences. Any applicant has to also present a record of one's criminal conduct. The SMA has confirmed that it also seeks information from any domestic counterpart supervisory authorities indicated by the applicant, as well as from the OMLP. This approach can limit the possibility of both criminals and their associates being appointed to a licence-holder's management or supervisory board, or being the BO of a qualifying shareholding.

243. The SMA also seeks to obtain information from its counterparts abroad. This was clearly illustrated in a case where to authorise an investment service provider, it sought information from seven (7) different authorities and only following the receipt and consideration of the same, did it consider that it was in a position to issue the necessary authorisation for the entity to carry out investment services and for different persons to acquire qualifying shareholdings in the same or take on their post on its supervisory and management boards.

244. The SMA, where necessary, requires further clarifications or additional documents from the applicant to supplement the original application. This has at times led to the application being withdrawn. Information on these cases is held by the SMA and is made available to other authorities and foreign counterparts should the need arise.

245. As regards ensuring that a licence holder and the persons involved with the same remain fit and proper, the SMA does not carry out any proactive checks itself but reacts to information brought to its attention. In this regard, it is to be noted that there have been occasions where the SMA took steps against persons that no longer met the conditions to be considered fit and proper. In one case, it prohibited two individuals from continuing acting as non-executive directors for one of its licensees after it resulted that these were subject to criminal investigation.

246. As to changes taking place after authorisation without the SMA being aware of them, any appointment to the management or supervisory board cannot be registered without the prior approval from the SMA. However, there appear to be no equivalent safeguards regarding the acquisition of qualifying shareholdings, or a change in BO, without the SMA's consent. The SMA has however confirmed that no such instances have taken place during the assessment period. This does not mean that the SMA does not take action should there be situations where this circumstance materialises as is also demonstrated through the following case example.

Box 3.2. SMA - acquisition of a qualifying shareholding

An individual acquired additional shares in shareholder resulting in its total shareholding exceeding the threshold to be considered as a qualifying holding. No prior authorisation was sought from the SMA but the individual divested part of the holding again within four days, bringing the holding below the threshold for being considered as a qualifying holding. Upon being informed of the case, the SMA considered whether there were grounds to take supervisory and enforcement action. While no supervisory action was taken as the breach was not deemed to be very serious and it was quickly remedied, the SMA did initiate a misdemeanour procedure against the individual which resulted in a warning.

ISA

247. ISA is authorising insurance undertakings, insurance intermediaries, and pension schemes. With regards to insurance undertakings and pension schemes, this includes authorising anyone wanting to acquire a qualifying shareholding in any of the afore-mentioned OEs as well as the members of their management board. Members of the supervisory board are not scrutinised prior to their appointment, though they are then subject to on-going scrutiny as set out in the following paragraph. Where the acquirer of the qualifying shareholding is a legal entity or arrangement, the ISA also takes into account and checks the standing of its BOs. The process followed by ISA in this regard is similar to that of the SMA. In the case of insurance intermediaries, the ISA assesses the fitness and propriety of their management and only in the event that there is a negative outcome does it also assess any qualifying shareholder. In a number of instances the individuals responsible for the management of the intermediary's activities would also be its BOs, limiting the negative impact of not looking at all qualifying shareholders, including their BOs.

248. Checks to ensure that fitness and propriety requirements are met on an on-going basis for insurance undertakings and pension schemes are carried out as part of the supervisory examinations held every three years. Between 2020 and 2024 it conducted on average six supervisory examinations a year where it also considered whether the members of the management and supervisory boards were still fit and proper. The frequency for checking qualifying shareholders and their BOs is however lower as this was only done in six visits, all carried out in 2022. While ISA licensees are expected to inform the ISA about changes in their status, the ISA can also react to information brought to its attention and carries annual off-site reviews to assess whether there were any changes to qualified shareholdings that were not notified to the ISA. 16 such checks are carried out annually, representing the total population of insurance, reinsurance and pension companies, on the basis of periodic reporting provided by the said FIs. Information on the current qualifying shareholders is also checked against the Slovenia Business Register, and an assessment of the shareholders' financial stability is carried out, including any publicly available adverse information or information otherwise known to the ISA. This led to the detection of at least two cases where issues with qualifying shareholdings were identified. Similar on-going checks are applied with regards to members of the management and supervisory bodies of insurance and pension companies.

249. With regards to insurance intermediaries, any change to their qualifying shareholders, management or supervisory boards, and to its beneficial ownership is not subject to any prior checks and approval by ISA. Intermediaries are expected to report these changes themselves on a periodic basis and it is then at this stage that the ISA checks whether fitness and propriety checks are being met. ISA has confirmed that there have been occasions where changes have not been reported, in which case it contacted the intermediary to obtain the necessary information. To address possible shortfalls in this regard, the Business Register communicates to the ISA changes to insurance intermediary companies for it to double-check against data obtained from the intermediary or on its records.

Box 3.3. ISA - acquisition of a qualifying shareholding

The ISA was informed that the BO of a qualifying shareholding, residing in another EU Member State, had been arrested by the authorities of the said Member State. Following obtaining clarifications from all the parties involved and seeking additional information through the OMLP, the ISA initiated a procedure to withdraw its approval to the individual in question to remain the BO of the qualifying shareholding and issued an order to the qualifying shareholder to divest itself of the shares held in the insurance company within a set period of time. The BO missed the deadline and therefore the ISA suspended the ability of the BO, through his holding company, to exercise the voting rights associated with the shares. A series of proposals were made to the ISA for the shares to be transferred to new shareholders but due to various reasons their application could not be proceeded with and the insurance company was eventually put into liquidation.

Ministry for the Economy

250. The Ministry for the Economy carries out some basic checks on individuals and entities that are to be involved with lending and leasing operators. While these checks are not exhaustive in nature, this is not considered as of major concern given the low materiality of these sectors.

VASPs

251. Until 30 December 2024, VASPs were subject to a registration process in Slovenia, with the OMLP being responsible for ensuring that the conditions at law for registration were met. The conditions in question included checks on the good standing of the applicant itself as well as, where applicable, on its legal representatives, directors, and beneficial owners. The same checks would be carried out with respect to Slovenian and foreign residents. These checks were limited to confirming whether the individuals involved with the legal person rather than the entity itself, had been finally convicted of a wilful crime or of specific criminal offences occasioned through gross negligence. While these checks could assist in determining whether one was fit and proper, these were not equivalent to the checks carries out in the case of a fully-fledged licensing procedure and, as can be seen from the case-study quoted hereunder, it is possible that these more rudimentary checks did not always prevent dubious operators from entering the market.

252. During this period, the BoS undertook a series of activities to identify possible cases where VASPs operating in or from Slovenia had failed to register with the OMLP. It did so by analysing information it received along with other publicly accessible information (e.g. records within the Business Register) as well as websites of operators that might have been subject to registration and other information from the internet. This led to a number of cases being identified and notified to the OMLP – 4 cases in 2021, 1 case in 2022 and 3 cases in 2023. These included cases where the application of the VASP for registration with the OMLP may have been still subject to processing, indicating that communication between the two authorities may have required some fine-tuning.

253. Responsibility for authorising VASPs under Markets in Crypto-Assets Regulation (MiCAR) has, of 30 December 2024, been vested in the SMA, with the BoS being responsible to authorise any of the already licensed credit institutions who want to also carry out VA services and act as issuers of e-money or asset-backed tokens. The checks carried out by the SMA when processing an authorisation application are similar to those applied when licensing an investment service provider as already described hereabove. Any VASP previously registered with the OMLP had until 1 July 2025 to either file an application to be so authorised or to otherwise cease activities. Anyone who so filed an application with the SMA could only continue servicing existing customers until such time as the SMA decided on its application. Out of 35 entities present on the register as at end of 2024, only 3 took advantage of the transitory period, with two being eventually

granted and one was refused.

254. The AT has been provided with the following case-study which shows the nature of the checks being carried out with respect to these applicants:

Box 3.4. SMA – licensing the VASP

The applicant was a VASP already operational in Slovenia on the basis of its registration with the OMLP, delivering its services through crypto-ATMs. The applicant filed its MiCAR authorisation application with the SMA one day before the lapse of the transitory period. Upon receipt the SMA formally notified that it could no longer on-board new customers. The SMA established that this was effectively being done through checks carried out on the applicant's website, on-site checks on one of its ATMs and also through checks on third party websites indicating the status of the crypto-ATMs.

In processing the application, the SMA sought information also from the BoS and the OMLP. Given that the main shareholder and the only director of the applicant was resident in another Member State, the SMA sought information from its counterpart in the said Member State which uncovered links between the said individual and criminal elements. On the basis of this information and on the basis that the individual in question was around eighty (80) years old, suggesting that he was acting as a strawman for someone else, the SMA refused the application.

255. Some minor concerns still persist as to whether enough is being done to ensure that anyone previously registered but who did not submit an application for a MiCAR authorisation has effectively ceased operations in or from Slovenia. The BoS has informed the SMA about possible cases where such VASPs may have ceased activities, and the SMA has carried out its own checks. Of the remaining 32, a number were already identified as not providing any services subject to MiCAR authorisation. This brough the total down to 26, with three being liquidated while a further 12 have not generated any revenue in the last years indicative of any on-going trading activity, 2 have moved their operations abroad while 1 has applied to also be authorised under MiCAR. 8 remain subject to further scrutiny by the SMA to determine their actual status, including some which are still showing signs of activity though this is not significant, and none had previously been rated as presenting a higher than medium level of risk.

256. In scrutinising potential VASPs the SMA is seeking information on already registered VASPs that applied for a MiCAR authorisation from different authorities, including the BoS and the OMLP as was also required in terms of the Action Plan following the 2025 NRA published this year. As also demonstrated by the case-study hereabove, the SMA is also running checks with its counterpart authorities abroad which is especially relevant within the context of a business that is not constrained by geographical boundaries.

3.2. Supervisors identifying understanding and promoting FI and VASP understanding of ML/TF risks

3.2.1 Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of FIs and VASPs and of individual FIs and VASPs over time

257. Overall, authorities had demonstrated an effective understanding of sectoral risks faced by FIs and VASPs which was developed through their participation in the NRA process. While all the main AML/CFT supervisors have a risk assessment process in place for their OEs, the depth of these varies, leading to more thorough risk comprehension in the material sectors

BoS – Sectoral Risk Understanding

258. The BoS has developed a robust methodology for the carrying out of sectoral risk assessments, the last version of which was adopted in 2025. It has also developed PAMLS – Platform for AML Supervision – an advanced IT tool for, amongst other things, detecting new and emerging risks through the AI-led analysis of transactional data. This is intended to allow the detection of emerging risks, trends and typologies at the sectoral and entity level. For the time being, PAMLS is used only with regards to banks though the BoS has signalled that it is looking at extending its use to the non-banking sector as well.

259. As to the actual carrying out of a sectoral risk assessment, the BoS has only carried one in 2022. This does not provide an analysis and understanding of the main and/or emerging ML/TF risks within the different sectors falling under the BoS' supervisory remit. It rather presents a summation of the results from the different entity-level risk assessments. Currently, this analysis lacks an adequate set of data sources and does not identify the possible threats.

260. This notwithstanding, it is acknowledged that the BoS has drafted the relative chapters in the NRA addressing the sectors falling within its supervisory remit and these can, to a large extent, be equated with sectoral risk assessments. However, given the lapse of time between the two NRAs (from 2020 to 2025), and the lapse of time since the data on which the respective NRA was based had been collected and the issue of the NRA, the trends identified through the respective NRA may not have been fully reflective of the actual threats and vulnerabilities within the sectors at the time of its finalisation. While this may be more relevant with reference to the banking sector, being the most sophisticated sector under the BoS' supervisory remit, it has to be pointed out that the sector is also relatively static and limited in terms of both operators and the products and services offered.

261. In addition, it has to be borne in mind that the BoS has to internally justify its supervisory plans on the basis of a sectoral explanation of the ML/TF risks it is noticing so as to have them approved. And while this risk understanding would largely be based on information sourced and held by the BoS itself, it also makes use of the EU's Supranational Risk Assessment and of the ML/TF Risk Opinion issued by the European Banking Authority to keep abreast of emerging threats and vulnerabilities which may not be currently noticeable within the Slovenian market but may eventually present themselves.

BoS – Entity Level Risk Assessment

262. The data sources considered for the carrying out of the risk assessment at entity level are multiple, key amongst which is the annual questionnaire that FIs falling under the BoS' remit have to complete. The BoS has advised that there is a 100% compliance rate in this regard. The questionnaires are quite thorough though there are aspects which are not explored or are only in part touched upon. This is especially true with regards to banks.

263. Given their key role within the Slovenian financial and AML/CFT system, the questionnaire would benefit from the inclusion of additional questions on legal persons and their BOs, the latter being an aspect that is only touched upon within the context of PEPs. There are no questions as to the presence of customers with complex ownership structures, the residence of BOs, how prevalent are certain types of legal persons amongst the customer base such as limited liability companies and NPOs. One has, however, to appreciate that most legal persons serviced by banks are locally registered or incorporated and have a mostly Slovenian beneficial ownership. Another aspect that is somewhat missing is that dealing with correspondent banking, a service in relation to which there are no questions in the annual questionnaire. And there are equally no questions on outsourcing, though this may not be particularly a feature within the Slovenian banking sector. In terms of controls and given the issues with backlog of flagged transactions to be scrutinised, the controls section of the questionnaire would benefit from questions as to the number of flagged transactions being

produced by the transaction monitoring system, how many have been processed and how many actually eventually led to a report to the OMLP. This would enable the BoS to have a better understanding of individual banks' effectiveness in this area.

264. The questionnaires for the non-banking sectors are equally good, enabling the BoS to obtain quite a range of data points that are of relevance in better understanding the different sectors. Questions on legal persons and BOs are equally missing from these questionnaires, though the incidence of legal persons in these sectors may actually be significantly less than within the banking sector. However, what has been stated previously with regards to outsourcing and flagged transactions would equally apply in this case. In addition, given the possible higher vulnerability of these sectors to TF, there might be the need to better distinguish between remittances or payments linked to jurisdictions considered to be exposed to higher TF risks as against those that are more exposed to ML risks.

265. Additional sources that complement and counter-balance information collected through the self-assessment questionnaire includes information available to the BoS through its different supervisory and prudential activities, information obtained from its counterparts, information from PAMLS (limitedly to banks) and information from the OMLP. The assessment process itself is partly automated as the questionnaire replies provided by the banking sector are collected through PAMLS and are then considered to see whether the additional information available to the BoS warrants an increase of the risk result produced by the said system. On the other hand, the non-banking sector's risk assessment process is fully manual, thereby imposing further demands on the bank's available resources. The subjectivity inherent in the use of supervisory judgement to finalise or revise the risk assessment in the circumstances referred to in para. 270 hereunder is mitigated through.

266. In the event of material changes occurring between risk assessment cycles, the BoS has a mechanism to revise the entity-level assessment to reflect the latest risk status.

SMA

267. The SMA is in the process of adopting a methodology for the carrying out of a sectoral risk assessment and is still to carry out a proper sectoral risk assessment. While it has explained that it has a holistic overview of the different operators through the entity level risk assessment process and its supervisory processes, it is also true that there is no dedicated periodical exercise to systematically risk assess the whole sector. This is usually a key exercise to identify emerging trends and risks. As is the case with the BoS, the SMA is also responsible for carrying out the risk assessment of the sectors under its remit for NRA purposes. Thus, even in this case, the absence of a proper sectoral risk assessment is mitigated through the NRA analyses, which however present the same shortcomings referred to earlier for the BoS.

268. The SMA carries out an annual risk assessment for the different FIs under its remit, the basis of which is the risk assessment questionnaire which has to be completed by the different OEs. As for the BoS, the SMA has confirmed that it has a 100% compliance rate. The questionnaire in itself is quite comprehensive, though it would benefit from additional questions on beneficial ownership, as this is currently only an aspect considered when it comes to the reasons for classifying a customer as high risk, complexity of ownership structures, payment methods used, and whether any of the BOs are PEPs. Other sources of information are also used, including those available to the SMA itself, but the process is entirely entrusted to the supervisory judgement of the SMA without any direction or guidance as to the weight to be attributed to particular data sources.

269. In the event that additional relevant information is made available during the year, the SMA would not revise the risk score per se until the next risk assessment cycle, but it would take actions to mitigate any perceived increase in the ML/TF risk of the OE.

ISA

270. The sectoral risk assessment for the insurance sector is based entirely on the NRA, which was carried out by the ISA itself. On the other hand, when it comes to the risk assessment at entity level, it carries out the same on the basis of a questionnaire that insurance undertakings and pension companies have to comply. In terms of the questions asked, the same issues as already highlighted for the BoS and the SMA arise.

271. It is to be noted that insurance intermediaries, i.e. agents and brokers, are not risk assessed as the ISA considers that they present the same risk as their principal. That could be argued with regards to insurance agents, but brokers are independent from single insurance undertakings. This notwithstanding, it is not considered that this impacts the risk understanding of the ISA, given the overall low risk of the insurance sector in general and the relative reliance on domestic insurance undertakings to source insurance products.

Market Inspectorate

272. The Market Inspectorate is supervising lending and leasing operators. The Market Inspectorate has no methodology for risk assessing leasing and lending companies, and over the assessment period has not been collecting data and information in a systematic manner so as to allow it to develop a proper risk understanding of leasing or lending companies. However, given the size and risks of the sector, this is not considered to be a major shortcoming.

3.2.2 Promoting FI and VASP understanding of ML/TF risks and AML/CFT obligations

273. In general, both FIs and VASPs confirmed that AML/CFT supervisory authorities are very accessible and willing to discuss practical difficulties that they encounter when it comes to the implementation of AML/CFT requirements. This serves as an additional channel through which the authorities enhance their guidance and outreach efforts. Furthermore, it is worth noting that there is a significant level of collaboration between authorities in both developing guidance and coordinating training events.

BoS

274. The BoS has been especially active in providing guidance and training to the FIs falling under its remit. It has issued a comprehensive set of Guidelines on the application of AML/CFT obligations to its FIs, which it updates from time to time in consultation with the SMA, the OMLP and the private sector, and has also adapted a series of EBA Guidelines within the national framework, including guidelines on risk factors and associated mitigating measures, and guidelines on the implementation of the Travel Rule. The BoS also issues Circular Letters, summarising the results of the thematic examinations and good practices which may have emerged from the same. These have included but are not limited to a Circular Letter addressed to banks on the risks presented, and the mitigating measures to apply when dealing with VASPs or VA-related services (2021) and one addressed to VASPs offering ATM services on the prevention of anonymous transactions (2022). Thus, the BoS does regularly communicates its regulatory expectations in writing to OEs under its remit.

275. While the BoS does not organise its own training events, it is a regular participant to training sessions organised by the Banking Association, such as its annual conference. While primarily aimed at banks, these training sessions are also attended by representatives from other sectors. In addition, the BoS has over the assessment period held a series of meetings with FIs and VASPs, either upon request of the OE – 7 – or as part of its supervisory activities – 18.

SMA

276. The SMA has issued a comprehensive Guidance Document on Risk Assessment and AML/CFT Obligations addressed to the sectors under its responsibility, which is updated from time to time whenever there are legislative changes and are accessible through its website. The SMA does not usually hold its own training events but is a regular participant in training events organised by industry representative bodies such as the annual conference organised by the Investment Firms Association and that organised by the Banking Association. This approach is understandable given the limited resources it has available to it for AML/CFT purposes. This notwithstanding, it is relevant to point out that the SMA has also held a training session for VASPs in 2024 in preparation for its assuming responsibility for this sector, as well as inviting anyone who files an application for authorisation as a VASP for a meeting where it also explains what its regulatory expectations are, including when it comes to AML/CFT.

ISA

277. The ISA has not been particularly active in providing guidance to FIs falling within its remit. It has issued Guidelines for ML/TF Risk Assessment, which are also accessible through its website, but these focus especially on the carrying out of the enterprise-wide risk assessment and only minimally touch upon the other AML/CFT obligations. No training sessions have been held for the insurance sector due to the low-risk rating attributed to this sector. There is still an element of outreach through the interactions had with the insurance representative body and with the communication of supervisory aspects of interest at the beginning of the year. This can ultimately result in undermining the sector's understanding of its AML/CFT obligations and lead to an uneven application of requirements.

Market Inspectorate

278. The Market Inspectorate has issued revised guidelines in March 2024 for credit providers and credit intermediaries. It has not provided any additional material, nor has it held training or outreach initiatives for credit providers and intermediaries.

3.3. FI and VASP understanding of existing and evolving ML/TF risks

279. All FIs and VASPs agreed with the analyses of their respective sectors in the NRA and the results of the said analyses. Understanding of ML/TF risks is generally well-developed, with stronger awareness in sectors facing more complex or specialised risk exposure.

FIs under BoS Supervision

280. FIs supervised by the BoS generally demonstrated a good understanding of the ML/TF risks they are exposed to, especially when it comes to banks and EMIs. They were all aware of the results of the NRA and considered that there were no additional risks to be added. They all referred to potential risks like non-resident customers with no links to the jurisdiction, complex ownership structures with foreign BOs, and cash as possible risks to which they may find themselves exposed. Specialised banks offering trade finance services were particularly aware of the risks associated with their particular activities and have implemented mitigating measures associated with the same. EMIs were particularly aware of the risks associated with innovative products like Virtual IBANs, with the only EMI to offer the said product having discontinued doing so as the associated risks were not easily mitigated. Banks and EMIs were especially aware of how particular typologies that could be indicative of ML/TF can manifest themselves within their respective sectors.

281. The annual risk assessment questionnaire as well as the questionnaire circulated for NRA purposes further assists FIs to understand the ML/TF risks they are exposed to, though this may not be sufficiently

detailed to allow a proper risk understanding by the FI compiling the same. As for the BRA, the main FIs could clearly articulate possible trigger events that would lead to a revision thereof, including the potential introduction of new products and/or services. BRAs are considered by the BoS in the context of its supervisory activities and were part of a thematic examination on four (4) banks undertaken between 2022 and 2023, the results of which were not in their majority considered serious enough to warrant enforcement action.

FIs under SMA Supervision

282. Both investment services providers and operators within the funds sector were aware of the results of the 2025 NRA and were largely in agreement with the ML/TF risks resulting therefrom. Fund management companies were especially aware of how collective investment undertakings managed by them could be vulnerable to ML/TF, including through subscription in kind and the presence of nominee shareholders, which they do not accept. Cash in particular was not something they would entertain as a means to effect an investment operation. VASPs were well aware of their ML/TF risks arising from the use of VAs having privacy features and from unhosted wallets.

FIs under ISA Supervision

283. Insurance undertakings and pension companies were very much aligned with the 2025 NRA when it comes to their risk understanding. They were able to articulate possible risks associated with their sector, including cash, the assignment of beneficiary rights etc. and provided a good explanation of how these can be mitigated. The same goes with the insurance intermediaries, though admittedly they are very much dependent on information provided by and mitigating measures communicated to them by their principal.

FIs under Market Inspectorate Supervision

284. Leasing and lending companies demonstrated a satisfactory understanding of the ML/TF risks to which they are exposed to according to the NRA.

3.4. FI and VASP understanding and compliance with AML/CFT obligations and mitigating measures

3.4.1 CDD, record-keeping, BO information, ongoing monitoring

285. FIs seem to have a good grasp of their AML/CFT obligations. In terms of customer on-boarding, most FIs still rely on obtaining hard copies of identification documents, with just a few of them relying on electronic on-boarding solutions. There is generally a good understanding of BO-related obligations, taking into account not just shares and voting rights, but also control via other means. Most FIs, especially banks, did report that they do encounter issues in verifying ownership and control structures involving foreign elements and/or resulting in a foreign BO due to the absence of reliable means how to do so or, where they exist, the costs involved. There is in general a certain degree of reluctance in servicing non-resident customers.

286. Most FIs also have sound procedures when it comes to on-going monitoring, with banks and EMIs that process considerable volumes of transactions adopting automatic screening tools. These are usually reliant on scenarios developed by the supplier and complemented by additional ones that are more in line with the business trends of the particular FI. These scenarios are revised regularly to determine whether they are still current, especially where they are producing a significant volume of false positives.

3.4.2 Enhanced or specific measures

287. FIs have demonstrated that they have a good understanding of the EDD measures to be applied in specific cases like PEPs and correspondent banking relationships. They also adhere to the list of high-risk jurisdictions issued by the OMLP but do also carry out their own independent checks to establish whether non-listed jurisdictions present higher risks.

3.4.3 AML/CFT reporting obligations, tipping off

288. Meetings with FIs and VASPs confirm that they have an understanding of their reporting obligations when it comes to suspicions of ML/TF. The overall reporting trend is aligned with the materiality of the respective sectors, with banks, PSPs and MVTS being responsible for the bulk of the reports received by OMLP. The exception is with VASPs where one would expect a higher number of submissions. While lower numbers are to be expected in less material sectors, it is still questionable whether the reports submitted by the investments and insurance sectors are reflective of their respective importance. However, when it comes to actual reporting the findings from supervisory engagement and the reports submitted to the OMLP show that there are practical issues in this regard. (See Table 6.1 in Chapter 6).

289. The largest share of reporting is to be attributed to banks, followed by MVTS and PSPs, all of which are OEs falling under the BoS. This is not to say that these sectors do not present issues when it comes to reporting. Attempts have been made to tackle defensive reporting, especially when it comes to MVTS as most reports related to TF but were triggered due to possible negative connotations associated with particular names without there being any actual suspicion. Indeed, there were no further disseminations made by the OMLP on the basis of these reports. While numbers have decreased, TF-related STRs are still featuring heavily within this particular category.

290. On the other hand, reports submitted by banks seem to be of better quality though the volume of reporting has been somewhat constant over the years. BoS supervisory activity did uncover instances of failures to report or of significant backlogs of flagged transactions that were not scrutinised for possible indications of ML/TF. These were attributed to issues involving the monitoring tools used and the resources available, in terms of both number and quality, to scrutinise the alerts generated. These issues were noted over the period 2020–2024. While remedial actions have been undertaken and there has been an increase in reporting for 2025, not enough time has passed to assess whether the said remedial action has had lasting effects in this regard. In addition, it is not clear whether within the same sector there may instances of under-reporting by specific operators.

291. Reporting levels by the investment services sector and by the insurance sector are considerably low, though the 2025 NRA does contain statements that condone the said reporting levels.

292. All FIs were also aware of their tipping off obligations. Neither the FIs and VASPs met on-site nor the authorities could remember there having been any tipping off cases.

3.4.4 Internal controls, procedures and audit to ensure compliance

293. All FIs indicated that they have some form of internal controls and procedure, though these do at times vary depending on the size of the OE in question. The more sophisticated FIs do recognise and carry out audits of their internal controls to ensure that they are suitable, having also clear procedures as to how findings resulting from the same are to be handled and what is to be the involvement of their respective managing and supervisory bodies within the whole process.

294. Insurance intermediaries are an exception as they do not have their own policies and procedures but rely instead on those of the insurance undertaking, they have a relationship with. This approach is understandable when it comes to insurance agents, as they are an extension of their insurance principal, but the independence that should characterise insurance brokers means that they should have their own policies and procedures. Equally, when it comes to internal audits, they do not carry out their own internal audits but rely instead on those carried out by their principal.

3.4.5 Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

295. The AT did not identify any legal or regulatory obstacles to the implementation of AML/CFT obligations and mitigating measures.

3.5. Supervisors risk-based monitoring or supervising compliance by FIs and VASPs

BoS

296. The BoS has a risk-based supervisory strategy in place, setting out the frequency with which FIs falling within particular risk bands will be considered for supervisory examinations and the possible types of examination to be carried out. This varies also on the basis of the sector in question, with the frequency being higher in the case of banks. The overall cycle for the banking sector spans six years, during which all those institutions presenting a Moderate, Significant or Very High ML/TF risk should be subject to some form of on-site supervisory engagement at intervales of six, four and two years respectively. The cycle for the non-banking sector is somewhat longer as it spans a total of seven years for the same risk-categories at intervals of seven, five and three years respectively. In either case, FIs calling within the Low-Risk band, which would include all currency exchange offices, are only to be subject to supervisory engagements when considered necessary by the BoS. The duration of each cycle is judged to be somewhat too long, given that the majority of the FIs falling under the BoS' supervision fall within the Low or Moderate categories. In addition, follow-up examinations are considered on a par with full-scope or thematic/targeted examinations, notwithstanding their more limited extent and focus.

297. The BoS has limited resources with which to supervise the FIs and, until July 2025, the VASPs falling within its supervisory remit. As at end of December 2024, it had only 3 FTEs to supervise a total of 30 FIs and 28 VASPs (though only 9 were active). The result is that the BoS is not managing to adhere to its supervisory plans, a vulnerability that was also identified in the 2025 NRA and in relation to which an action point was set out in the resulting Action Plan.

298. In the evaluation period, in total, BoS carried out full-scope and thematic on-site examinations on 73% of the banking population, representing approx. 96% of assets within the banking sector. The use of thematic examinations is especially visible when it comes to the banking sector, with 3 thematic on-site examinations having been carried out over the assessment period covering a total of 14 institutions, as against only four full-scope examinations having been carried out between 2020-2023 and none in 2024. These were not always the examinations carried out on the riskiest banks as in two instances there were banks with a higher risk profile that were subject to a thematic examination instead. However, in those cases a full-scope examination had just taken place while the other was undergoing remediation and was the subject of a follow-up examination. On the other hand, while thematic examinations can provide a good snapshot of what risks and mitigating measures an institution or sector is applying in a given area, they do not provide a comprehensive overview of the whole AML/CFT framework of the particular institution. Moreover, this tool has been used to mostly assess the implementation of requirements arising from recently

introduced legislative or regulatory changes and does not seem to have taken into account high risk areas highlighted by the NRA (e.g. correspondent banking).

299. Indeed, the BoS preferred supervisory tool is the thematic examination, with a total of eight such examinations carried out between 2020–2024 covering institutions, banks and non-banks, having a moderate to a high-risk profile. It is interesting to note that within the non-banking sector, the thematic examinations are quite comprehensive and come close to full-scope examinations as they relate to how higher risk non-banking entities comply with the overall spectrum of their AML/CFT obligations. Three of these thematic examinations related to VASPs, which at the time fell under the BoS supervisory remit.

300. Intervals between examinations do not entail that there is no interaction between the OEs and the BoS as there are other touchpoints in place, including questionnaires and management meetings.

301. The procedure for the carrying out of on-site examinations is set out in the BoS' Operational Guidelines, which set out what are the different supervisory tools available to the BoS and how they differ one from the other, and Rules of Procedure for Inspections. The Rules of Procedure for Inspections regulate in detail the actual procedure to be followed for the carrying out of on-site examinations. There is, therefore, in place a set procedure for the carrying out of supervisory examinations and these tend to be quite thorough and extensive as also informed by different OEs. In all instances, prior to the carrying out of supervisory engagements, the BoS seeks the input of the OMLP in terms of the level and quality of reporting by the particular FI or, until it was responsible for them, VASP. The results of the examination are communicated to the OE through Supervisory Letters or Orders to Comply and are quite detailed, setting out what was finding, the obligation concerned and also what is expected of the OE in terms of possible remediation.

302. Notwithstanding the difficulties and limitation highlighted above, the BoS also seeks to carry out group-wide supervision of FIs that have cross-border operations in cooperation and coordination with its counterparts in other jurisdictions. Indeed, it did have one such instance which it carried out in conjunction with its counterpart authorities in Bosnia and Herzegovina and North Macedonia. In addition, it regularly shares its findings from its supervisory activities with other interested counterparts.

SMA

303. The SMA had, at the end of 2024, 60 FIs under its supervision – 51 AIFMs, 5 UCITS management companies and 4 investment services firms. Actual supervisory activities on these FIs are carried out by 2 FTEs focused on the investment services firms and 2 FTEs focused on the fund management companies (and indirectly the collective investment schemes they manage). The SMA has, as of July 2025, been vested with responsibility also for the AML/CFT supervision of VASPs. While the number of eventual VASPs falling within its supervisory remit has still to be defined, no additional resources have been made available to cater for this new cohort of OEs.

304. The SMA has a general risk-based supervisory strategy which, while recognising that OEs that are assessed with a higher risk of ML and TF are subject to more frequent and in-depth supervision, does not set out which supervisory tools are to be used with respect to specific risk categories. It's supervisory planning seems to be dictated more by the resources available to it as it seeks to carry out at least an on-site thematic examination on 1-2 investment services firms and on 1-2 collective investment schemes on an annual basis, independently of the level of risk they present. While thematic examinations allow a more focused approach to OEs' risk control framework, they do not allow for a holistic appreciation of a control framework's effectiveness.

305. In terms of the carried out supervisory activities, no full scope on-site examinations were held in 2020-2024 and 8 thematic on-site examinations were otherwise held during the review period. It has to be noted that these thematic examinations do not target a specific area of ML/TF risk or aspect of the AML/CFT

control framework, but come close to being full scope examinations as they take into account the adequacy of the ML/TF risk assessment framework, CDD measures including transaction monitoring and reporting to the OMLP. None of the licence holders selected for on-site examinations, nine in total, were rated higher than Medium Low in terms of ML/TF risk, even though throughout the review period there were on average fourteen licence holders rated as presenting a Medium level of ML/TF risk and at least one licence-holder that was rated as Medium High. 2023 has seen a gradual escalation in terms of the level of ML/TF risks presented by licence holders compared to earlier years but this did not lead to full scope on-site examination in those entities. These higher risks rated OEs were instead the subject of off-site examinations, a less intrusive and intensive supervisory tool than the thematic or full-scope on-site examination.

306. The SMA also makes use of off-site thematic examinations, consisting in assessing whether there are any changes from one year to another as to the information provided through the annual risk questionnaire. However, it is questionable whether this is the best tool to assess compliance with AML/CFT obligations within the higher risk-rated (medium-high) categories.

307. As to the actual carrying out of any on-site examinations, these were described by both the SMA and the OEs as being quite intensive.

ISA

308. The ISA does not seem to have a supervisory strategy in place. However, it has consistently risk rated insurance companies as low risk and, in practice, carried out full-scope examinations on the said companies once every three years. Insurance intermediaries are also subject to supervision, though there have been only 54 such examinations over the assessment period.

Market Inspectorate

309. The Market Inspectorate does not have a supervisory strategy. The annual inspection planning is based on the available resources rather than other factors. Thus, the Market Inspectorate undertook 13 on-site supervisory interventions on non-bank lenders in 2022, in 2023 and 21 in 2024. Inspections are conducted per available guideline for supervision and do not differ from entity to entity. The onsite visit lasts from half to one day and consists of checking 3 customer files. Internal documents of the supervised entity are gathered and analysed at the inspector's desk. The overall length of the inspection is not clear since the inspectors deal with multiple tasks at a time. It can be concluded that the shortage of resources hampers the abilities of the Market Inspectorate for an effective risk-based supervision. While infringements were noted in 6 of the supervisory engagements carried out, the absence of more granular statistical data for the period 2020–2024 does not allow the AT to make any assessment as to the adequacy of what supervisory activities are undertaken by the said authority.

OMLP

310. The OMLP is a secondary supervisor for FIs and VASPs, and therefore carries out limited supervisory activities, albeit complementary to the supervisory activities carried out by the other main FI supervisors. Its supervisory activities are more targeted in nature, acting upon particular information it may receive internally from the other sections of the OMLP or from sources like the media. In total it has carried out four targeted examinations on banks and two more general on-site supervisory examinations on leasing companies. Considering the additional responsibilities that the OMLP's supervisory team has to meet, this may be the best use of these additional but limited resources.

Cooperation between Supervisors

311. The limited resources available to supervisors makes the need for cooperation and collaboration between the authorities more indispensable. To address this issue, a joint commission - Commission for

Cooperation between Supervisory Authorities on the Planning of Joint Supervisory Procedures – has been established. Bringing together the BoS, the SMA and the ISA, representatives from the three (3) supervisors meet at the beginning of the year to discuss their intended plans for AML/CFT supervision and the supervision of other areas. Unlike what its name suggests, the said forum is more used to communicate information about possible supervisory plans but not to actually plan or revise plans to widen and deepen coverage of FIs falling within the supervisors' respective remit. As to actual joint examinations, these are at times carried out between the SMA and the BoS on banks carrying out both banking and investment services. However, this is quite exceptional in nature.

3.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on FI and VASP compliance

312. Authorities have a number of measures that they can apply where they detect shortcomings in the application of AML/CFT obligations. Measure of a supervisory nature include undertaking remedial actions with varying degrees of follow-up assessment, restrictive measures and, in more serious cases, the ability to withdraw authorisations to either conduct licensable activities and/or hold particular positions within FIs and VASPs. Remedial actions are tested through follow-up activities of varying degrees and overall seem to achieve the desired results.

313. Punitive measures consist in warnings and/or pecuniary penalties imposed through the misdemeanour procedure under the Minor Offences Act, i.e. an action of a criminal nature. It is to be remarked that the misdemeanour procedure presents a number of aspects that may not be conductive to sanctions that are in effect proportionate, effective or dissuasive, these being:

a. The authorities can only undertake a misdemeanour procedure where they have also identified an officer of the FI or VASP who can be considered as liable, together with the FI or VASP, for the alleged breach.

b. The payment of the pecuniary penalty imposed within eight days of its imposition without recourse to the law-courts results in an automatic 50% decrease in the penalty.

c. A four-year prescriptive period is to be applied when supervisory authorities' misdemeanour procedures are appealed from. This can result in the actions of the authorities being reduced to nought and quite serious breaches going unsanctioned. By way of example, in one particular instance the BoS had decided to impose a EUR 49 000 EUR fine on a bank, a EUR 1 300 fine on one of its responsible persons and a warning on another responsible person but in judicial review the court could not proceed further and had to strike down the BoS decision as the statute of limitations had run its course.

314. All misdemeanour procedures which result in the imposition of a pecuniary sanction and/or in a formal warning are published on the website of the authority in question.

315. Breaches of AML/CFT obligations are categorised by the APMLTF-2 according to their importance and severity, providing discretion to the authorities as to the pecuniary sanction to apply within a specific min. – max. range. All three authorities lack specific procedures laying down the criteria to be taken into account to determine the quantum of the pecuniary sanction and the actual quantum thereof, with authorities relying instead on past experience. Equally absent are detailed guidelines supplementing the general criteria set out in law for the determination of whether the misdemeanour procedure is to result in a warning or a pecuniary fine, though the BoS has indicated that warnings are mostly applied for first time offenders or less severe breaches. This provides for a degree of subjectivity which may not always lead to the imposition

of proportionate, dissuasive and effective sanctions taking into account the breaches that would have occurred.

316. The absence of data as to the nature of the findings that were dealt with through informal and formal means of remediation acted as a limitation on the AT part to assess whether it was proportionate to deal with the said findings just through remedial measures without the need to also apply punitive measures.

BoS

317. The supervisory activities of the BoS usually result in at least so-called Supervisory Letters, which are informal supervisory measures targeting findings that the BoS considers as being lesser shortcomings, i.e. findings that are less serious and in relation to which it would anyway have provided some form of recommendation. More serious findings are usually subject to an Order to Remediate, which is a formal supervisory measure.

Table 3.1 Statistics on Supervisory Outcomes within the Banking Sector

Year	Supervisory Measures	AML/CFT Infringements	Remedial Measures	Supervisory Letters	Lesser shortcomings	Recommendations
2020	3	10	6	8	17	25
2021	1	2	3	10	12	16
2022	2	4	12	3	5	6
2023	2	7	9	6	19	31
2024	0	0	0	3	8	13
Total	8	23	30	30	61	91

318. The statistical data provided does not allow to determine whether the findings resulting from supervisory activity are decreasing in terms of seriousness. On the other hand, Supervisory Letters and Orders to Remediate do allow an appreciation of how the BoS exercises its discretion as to which findings are to be addressed through one rather than the other. This determination is left to the discretion of the BoS' AML Supervision Team, acting on the basis of past experience and generic criteria found in law. Factors taken into account include the seriousness of the obligation breached, the nature of the business carried out by the FI as well as its relative size, the systematic nature or otherwise of such breaches, and whether any remediation may have already been undertaken.

319. Independently of whether the remedial action ordered is formal or informal, the BoS requires the submission of a detailed remediation plan by the OE and the submission of a final declaration with evidence that the remediation has been completed. The BoS supplements the information provided by the OE with follow-up examinations. Remediation is usually carried out within the set timeframes. In those sporadic instances where this does not take place, the BoS applies ever more intrusive examinations. This can be seen in two cases as follows. In one case, a VASP was subject of thematic examination in 2021, two follow-up examinations in 2022 and 2023, and a full scope on-site in 2024 which revealed further serious issues. The case was concluded from a supervisory perspective due to the VASP notifying the BoS that it was intent on ceasing activities. In another case involving a bank, supervisory action was undertaken in 2021. The on-site inspection that identified shortcomings was carried out in 2022, with two follow-up examinations being carried out in 2023 and 2024 when the issues identified were finally resolved.

320. The BoS has also undertaken misdemeanour procedures against OEs where it considered that there were sufficiently serious findings. This has happened in eight instances, including in a case involving a VASP. In one case, a bank was imposed a EUR 900 000 fine for failure to report cash transactions and transactions linked to a high-risk jurisdiction in 223 instances, in another it imposed a fine for EUR 137 000

for systematic breaches of key AML/CFT obligations (adequacy of the reporting officer, of the risk management policies and procedures, application of EDD measures etc.). These two cases demonstrate the ability of the BoS to calibrate its pecuniary sanctions to the seriousness of the case, taking into account the nature and the number of breaches.

321. A factor that may be undermining the effectiveness of the BoS enforcement actions, is the possibility under the misdemeanour procedure to have any pecuniary penalty decreased by 50%. While one appreciates that this can avoid the process being further extended to take into account judicial proceedings and limit the burden on the law courts, the prescriptive nature of this measure results in the penalties being applied eventually not being proportionate, effective or dissuasive when considering the seriousness of the breaches for which they were imposed.

Table 3.2 – Penalties vs Breaches

Sector	Breach	Penalty Imposed	Penalty Effectively Paid
VASP	Failure to provide information to the BoS	EUR 6 000	EUR 3 000
Bank	Failures related to the application of EDD and transaction monitoring	EUR 137 000	EUR 68 500
Bank	Failure to remedy deficiencies Failure to submit an STR in four instances	EUR 78 000	EUR 39 000

322. As stated, the misdemeanour procedure requires that there be identified one or more officers to undertake the said procedure vis-à-vis the OE and the said officer as well. The BoS has indeed sanctioned such individuals, but the said procedure is conductive to higher degree of compliance only if it results in sanctions that are effective and dissuasive. Considering the amounts that can be imposed by way of fines and the amounts that are imposed, this is questionable at most. In one case, the OE was subjected to a EUR 900 000 fine but the responsible officers only received fines totalling EUR 3 000. In another instance the OE was subjected to fines amounting to EUR 218 000 whereas the responsible officers were subjected to fines totalling EUR 6 000 and a series of warnings. This is somewhat mitigated through the publication of the measures so undertaken.

SMA

323. The SMA equally relies on informal remediation when it determines that there are findings which it classifies as not being of a serious nature. There have been only two instances over the review period where the SMA has imposed remediation by means of an order. However, the absence of any proper internal guidance and of statistical data on findings that resulted in formal and informal remediation does not allow any determination as to whether the remedial action is having the desired effect.

324. Both in the case of informal and formal remediation, the SMA requires the OE to provide it with evidence that it has completed the remediation required of it. However, there is no follow-up examination carried out to establish whether the necessary corrective actions have been implemented in practice, with the SMA preferring to then verify what actions had been taken once the OE is again chosen for a supervisory engagement. The only instance in which it would consider carrying out a follow-up examination is in case it has doubts about the veracity of the information provided. In the absence of statistical data on the issues that are usually addressed through informal remediation as against formal remediation, it is difficult to state whether this approach is justified or otherwise.

325. No misdemeanour procedures undertaken by the SMA over the period 2019–2024 resulted in pecuniary fines, though there were a number of warnings imposed on OEs and their responsible persons. Taken in isolation, the breaches identified would justify the course of action chosen by the SMA. Information on these warnings was published on the SMA’s website.

ISA

326. The ISA has had even fewer occasions to exercise its sanctioning powers, there having been only one case where it effectively imposed remediation on an insurance company. Given that the case involved the absence of a system to determine whether a customer or, where applicable, its BO is a PEP, it can be questionable whether the absence of any misdemeanour procedure for a systematic breach can be considered as having been proportionate, effective and dissuasive.

Market Inspectorate

327. The MI has indicated that there have been occasions where it has imposed both corrective actions as well as had recourse to the misdemeanour procedure.

Table 3.3 Statistics on sanctions imposed by Market Inspectorate

Year	Number of undertaken inspections	AML/CFT Infringements	Remedial Measures	Written Warnings	Fines
2022	13	4	2	4	0
2023	1	0	0	0	0
2024	21	1	1	0	0

328. The MI also provided information on two cases where it had recourse to the misdemeanour procedure due to the infringements it noticed – in one case the FI was found not to have carried out its business risk assessment while in another it failed to prepare a training programme for its employees. In both cases it imposed a written warning even though one breach can be considered as more serious than the other. This raises questions as to whether the measures applied are actually proportionate to the severity of the infringements detected. On the other hand, the said infringements were remedied within less than a year.

Chapter 4. Non-financial Sector Supervision and Preventive Measures

The relevant Immediate Outcomes considered and assessed in this chapter is IO.4.[19] The Recommendations relevant for the assessment of effectiveness under this chapter are R.22, 23, 28, 34 and 35 and elements of R.1, 29 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Licensing and registration frameworks are present for DNFBPs in Slovenia, but their effectiveness is significantly affected by their administrative nature, lack of independent verification, reliance on self-certification, and major regulatory gaps. Market entry controls do not target prevention of criminals' associates from holding ownership or management positions. Detection of unauthorised entities is weak. There are no market-entry regulations set for tax advisors, accountants and DPMS (dealing in precious stones or raw precious metals). In addition, there is no clarity whether legal advisors (not registered with SBA) perform activities that fall under FATF Standards even though the 2025 NRA identifies the group as posing a higher ML risk.

b) Supervisors' understanding and implementation of AML/CFT obligations, as well as identification of ML/TF risks within DNFBP sectors in Slovenia, is generally weak. Most supervisors have not integrated NRA findings into their supervisory frameworks. Although some recent steps have been taken to assess sectoral and individual entity risks, so far, these efforts have not been comprehensive or effective. The FARS is an exception, demonstrating a greater understanding of ML/TF risks in the casino sector.

c) DNFBPs showed overall limited understanding of ML/TF risks, even in higher-risk sectors. Among those, casinos and internationally active accountants and auditors, demonstrated a higher awareness of the nature and the level of their ML/TF risks. Most OEs underestimated sectoral risks, seeing their exposure as low due to mainly local clients, few suspicious cases, and reliance on banks' AML/CFT controls. Although all DNFBPs must complete annual risk assessments, these are often treated as a formality and lack forward-looking analysis.

d) Casinos demonstrate comparatively stronger compliance due to well-developed internal controls, compliance frameworks, and regular on-site inspections. Covered lawyers, accounting and auditing firms linked to international networks generally show more advanced controls, supported by group-wide AML/CFT standards. Other DNFBPs have less developed AML/CFT frameworks, and whilst they could articulate the legal requirements, many were unable to explain how these would be applied in practice or provide examples of when they had been applied.

e) Supervisory authorities and SRBs have limited staff and budgets, resulting in weak supervision. Except for FARS, supervisors have not adopted risk-based approaches, instead basing efforts on

19 When assessing effectiveness under Immediate Outcomes 4, assessors should take into consideration the risk, context and materiality of the country being assessed. Assessors should clearly explain these factors in Chapter One of the mutual evaluation report under the heading of DNFBPs, as required in the instructions under that heading in the Methodology.

available resources and reactive measures rather than actual ML/TF risks. Incomplete information on the population of OEs, especially in real estate, DPMS, tax advisors, and accountants' sectors, further hampers effective supervision.

f) Supervisory authorities rarely impose financial penalties or make use of the range of available sanctioning powers. Most enforcement measures consist of written warnings or remedial action, with little to no follow up on compliance. Where sanctions are applied, they are modest, inconsistent, and lack deterrent effect.

g) With the exception of legal advisors, all other DNFBP sectors have been issued with guidance, and some training is provided by supervisors. However, these efforts are insufficient to address the issues noted concerning the low level of understanding of ML/TF risks and awareness of AML/CFT measures.

Key Recommended Actions (KRA)

a) Slovenia should conduct a comprehensive assessment of the legal advisors' sector to determine the activities and services provided by those. When those fall within the scope of the FATF Standards, Slovenia should (i) assess the ML/TF risks associated with the sector, and (ii) establish and implement regulatory and operational supervisory frameworks, including effective market entry requirements.

b) Slovenia should: (i) set registration or licensing frameworks and appoint a designated competent authority or SRB, for Tax Advisors, Accountants, and all types of DPMSs; (ii) considerably strengthen the market entry framework, including verification of information on criminal background (except for the casino sector), ongoing fitness and properness checks, and introducing checks on criminal association; and (iii) establish clearly documented detection and termination policies and procedures of unauthorised operators (except for the casino sector).

c) Slovenia should increase supervisory capacities, including human resources at MIRS, SRBs and the OMLP, and ensure a that ML/TF risks of DNFBPs are comprehensively identified, understood and regularly monitored, and that the risk-based approach is applied in supervision and monitoring.

Other Recommended Actions

a) DNFBP supervisors and SRBs (excluding FARS for casinos) should maintain an up-to-date understanding of sectoral ML/TF risks, including activity size, complexity, cross-border exposure, and client base. They should enhance quantitative data collection beyond self-assessments and establish mechanisms to ensure consistent, comprehensive, and comparable data gathering.

b) Slovenia should ensure that the DNFBPs (excluding casinos and entities within large international groups) strengthen CDD frameworks by incorporating robust customer and transaction risk assessments, independent verification of customer data and source of funds, and application of EDD measures, particularly for PEPs and higher-risk jurisdictions.

c) Slovenia should: (i) ensure legal and operational capacity of supervisory authorities and SRBs to obtain sector data and act on non-compliance; (ii) implement risk-based supervisory programmes and methodologies that incorporate multiple information sources (e.g. inspections, inter-agency data); (iii) strengthen supervisory frameworks - including a balanced mix of onsite and offsite activities; and (iv) strengthen the enforcement framework to establish comprehensive sanctioning policies and ensure penalties are proportionate, effective, and dissuasive.

d) All supervisory authorities and SRBs should implement structured training and outreach programmes to improve DNFBPs' awareness of ML/TF risks and AML/CFT obligations. This should cover sector-specific risks and typologies, cash risks, institutional risk assessments, CDD/SDD/EDD measures, and STR reporting procedures, including consent requirements where applicable.

Overall Conclusions on IO.4

The overall framework for DNFBP supervision and the implementation of preventive measures in Slovenia is weak. The supervisory framework is fragmented, inconsistent, and largely administrative, with weak market-entry controls and limited independent verification. Important gaps remain, including the absence of registration regimes for certain sectors and lack of clarity regarding the coverage of legal advisors, creating potential regulatory gaps.

With the exception of FARS, supervisors demonstrate a limited understanding of ML/TF risks and have not integrated NRA findings into their frameworks. Risk-based supervision is largely absent, with activities driven by available human resources rather than risk, further hindered by incomplete registers to identify OEs that fall within the scope of Slovenia's AML/CFT framework.

DNFBPs show a generally weak understanding of ML/TF risks and often underestimate their exposure. AML/CFT measures are implemented in a formalistic manner, with limited evidence of a risk-based approach in practice. While key obligations such as CDD and enhanced measures are understood in theory, they are not consistently applied. STR reporting remains extremely low with most DNFBPs preferring to reject clients rather than report suspicions.

Supervisory guidance, training, and enforcement are insufficient. Sanctioning is limited, inconsistent, and lacks deterrent effect. Although stronger compliance is observed in casinos and internationally affiliated entities, the overall effectiveness of preventing ML/TF misuse in the DNFBP sector remains limited.

There is also a potential area of concern regarding legal advisors (see the Introduction for further details). The limited understanding of this sector, including the nature and scope of activities performed, creates a potential regulatory gap and may result in parts of the sector operating outside Slovenia's AML/CFT framework.

Slovenia is rated as having a low level of effectiveness for IO.4.

329. The AT applied the following weighting to assess the implementation of preventative measure by DNFBPs: extremely important for Real Estate and Lawyers (Attorneys registered with the SBA and other lawyers), very important for Tax advisors, accountants, and dealers in precious metals and stones; moderately important for Casinos and Notaries; and less important for Auditors. The details of the weightings of each sector are to be found in Introduction.

330. With regard to Trust and Company Service Providers (TCSPs), Slovenia advised there is no registration framework for these types of entities. However, the activities that fall under the FATF definition of TCSP are conducted by other types of DNFBPs, namely lawyers, tax advisors, accountants and notaries. It should also be noted that, as identified in R.22.1, the definition of TCSP activities in APMLTF-2 does not fully comply with the FATF Recommendation.

331. The assessment throughout this IO does not include legal advisors who are not registered with the SBA. Slovenia has an inconsistent understanding of whether this sector falls within the scope of FATF Standards, and as a result, there is no supervisory framework for this sector, and these entities were not met during the onsite (see also introduction for further information). The lawyers registered with the SBA are referred in the report as "covered lawyers".

4.1. Licensing, registration and controls for DNFBPs preventing criminals and associates from entering the market

332. Several competent authorities and SRBs share responsibility for market entry controls across the DNFBP sectors. However, there are no designated authorities responsible for DPMS (except for registration of dealers of precious metal products, excluding the traders dealing in raw materials), Tax Advisors or Accountants, and therefore there are no market entry controls for these sectors.

333. With the exception of the FARS, none of the other authorities or SRBs have internal documents outlining the procedures governing market entry controls to prevent criminals from entering the market. Instead, they rely solely on the legal provisions contained within the respective sectoral legal acts, which e.g., prescribe the information to be submitted by applicants and is largely limited to the submission of criminal history certificates. Furthermore, no authority or SRBs (except for FARS and the MoJ) conducts ongoing assessments to ensure that DNFBPs continue to meet fit and proper requirements.

334. As noted in R.28, Slovenia does not have any legal provisions to address the prevention of association to criminals. This results in the absence of specific market entry controls addressing this issue across all DNFBP sectors.

335. None of the supervisory authorities or SRBs reported any cases in which a DNFBP licence or registration was rejected on grounds of ML/TF risks. Slovenian authorities explained that this was due to the explicit legal requirement that OEs must not have prior convictions, which likely deters ineligible applicants from applying in the first place.

4.1.1. Market entry controls

336. *Real estate* – The Ministry of Solidarity-Based Future is responsible for Real Estate agents (licensed natural persons) market entry controls. Only natural persons may be licensed to carry out real estate activities, while Real Estate entities (business entities or licensed natural persons with sole proprietor status) are permitted to operate only if they employ at least one licensed real estate agent. The Ministry of Solidarity-Based Future maintains the official registry of the licensed Real Estate agents, whilst Real Estate entities register within Slovenia's Business Registry.

337. Real Estate agent applicants are required to provide basic information on their identity, residence, education, and indicate whether the agent will be providing brokerage services for a real estate entity. This should be accompanied with information on their criminal background. The Ministry of Solidarity-Based Future independently verifies the criminal background information provided by applicants, including conducting checks with foreign counterparts, to identify or verify the criminal history of applicants who have previously resided outside Slovenia. The Ministry of Solidarity-Based Future does not conduct

ongoing monitoring of the fitness and propriety of the registered licensed real estate agents. There are no market entry controls on real estate brokers registering with the Business Registry.

338. *Covered Lawyers* – The SBA is responsible for the registration of covered lawyers (attorneys registered with the SBA). Entry into the register is granted if the applicant meets the conditions set out in the Attorneys Act. One of the key conditions is that the person must be deemed trustworthy to practice law, and this is confirmed through the submission of a criminal background report provided by the Slovenian courts. A person is considered untrustworthy if they have been convicted by a final judgment of a criminal offence that renders them morally unfit to perform their duties, or if their conduct warrants the reasonable conclusion that they will not practice law honestly and conscientiously. The registration process is based on self-certified information provided by the applicant, with no further independent checks conducted to identify any adverse information or other matters that could impact the fitness and properness of the applicant. If the SBA becomes aware that a covered lawyer has been convicted of a criminal offence, it may initiate appropriate proceedings to remove the individual from the register on the grounds of loss of trustworthiness. Otherwise, the SBA does not conduct ongoing monitoring of the fitness and propriety.

339. The SBA noted a number of examples where applicants voluntarily withdrew their application because the applicant realised throughout the process that it would not meet the "trustworthy" requirements. Furthermore, the SBA advised of 4 applications during the assessed period (2020-2024) that had been rejected. One example provided noted the receipt by the SBA of a negative opinion by a regional bar association, regarding the actions of a covered lawyer that was deemed to not be trustworthy following an investigation by the regional bar association, and the subsequent decision to disbar the covered lawyer.

340. *DPMSs* – The Metrology Institute is responsible for the registration of dealers of precious metals. There is no designated authority responsible for licensing of dealers in precious stones and in raw metals. Business entities operating as dealers in precious metals and stones are registered with the Business Register which is publicly available. Neither the Metrology Institute nor the Business Registry carry out any fit and proper checks.

341. *Casinos* – Concessions for the conduct of Games of Chance activities are granted by the Government of Slovenia, with support from the Ministry of Finance and FARS. A maximum of 62 concessions can be granted at any point in time, two for classic games of chance, 15 for special games of chance in Casinos, and 45 for the organisation of special games of chance in gaming salons. The Ministry of Finance is responsible for maintaining an accurate and up to date register of concessions granted, including data on the concession period and extensions granted. An applicant must provide information on its beneficial owners, shareholders, partners and management board, and CDD is thoroughly conducted on all parties. These checks require confirmation that none of the parties hold a criminal conviction. When conducting checks, information is verified independently using open-source data analysis tools and information may also verified with the OMLP. No checks are conducted to identify criminal associates.

342. Concessions shall be granted for a maximum of 10 years, although the FARS noted that the majority of concessions are granted for 5 years only. During the life of the concession contract, Casinos are required to obtain prior approval for any changes to its shareholding or beneficial ownership structure, or the removal and appointment of individuals within the management board. On receipt of an application for any of these events, the Ministry of Finance and the FARS will carry out comprehensive CDD to determine the fitness and properness of the individual(s). However, in the absence of such applications, no ongoing checks are done on BO or key individuals which may limit Slovenia's ability to identify criminals holding key functions, or associated with criminals, within Casinos.

Table 4.1. Applications processed by MoF and FARs on BOs and key individuals

	2020	2021	2022	2023	2024
Received	256	347	483	463	518
Approved	250	325	469	448	507
Rejected	0	5	0	0	0
Withdrawn by applicant	6	17	14	15	11

343. *Notaries* - The Ministry of Justice, with support from the CNS, processes the registration of notaries under the provisions of the Notary Act. The Notary Act outlines specific eligibility and suitability requirements that applicants must meet. The registration process primarily focuses on assessing the applicant's professional competence and integrity, with only limited consideration of AML/CFT obligations. Applicants must confirm that they have no prior criminal convictions through the submission of a criminal background report provided by the Slovenian courts, and this is verified by the MoJ. However, no independent verification checks are carried out to identify any other adverse information that may impact the fitness and properness of the applicant, including conducting ongoing checks.

344. *Auditors* – The Agency for Public Oversight of Auditing (APOA) is responsible for registration of auditors under the provisions of the Auditing Act that outlines specific eligibility and suitability requirements that applicants must meet. The registration processes primarily focus on assessing the applicant's professional competence and integrity, with only limited consideration of AML/CFT obligations. In most cases, the fit-and-proper assessment relies on self-declarations by applicants of no prior criminal convictions through the submission of a criminal background report provided by the Slovenian courts. However, no independent verification checks are carried out to verify the information or identify any other adverse information that may impact the fitness and properness of the applicant, including conducting ongoing checks.

4.1.2. Detecting and addressing breaches

345. With the exception of the FARS in relation to Casinos, none of the other supervisory authorities or SRBs have mechanisms in place to systemically and pro-actively monitor, identify or investigate DNFBP activity provided by unauthorised operators.

346. The FARS demonstrated pro-active and extensive efforts in detecting and disrupting illegal online casinos that operate in Slovenia. The FARS has clearly documented procedures outlining the steps taken, including issuing the operator with a written warning and the application to the Court for access restriction. Furthermore, FARS has established follow up procedures to confirm that that court-ordered access restrictions have been successfully enforced.

347. Whilst the MIRS does not have procedures to pro-actively identify unauthorised operators, it did provide an example that demonstrated its approach when information is received regarding such. The MIRS advised it received two complaints from the public against one real estate entity. The MIRS' initial assessment suggested that the real estate entity was operating without a registered real estate agent, prompting the initiation of an inspection. The real estate entity remediated its position, and the MIRS issued a EUR 12,500 fine for the contravention. However, reliance on ad hoc complaints rather than proactive detection mechanisms does not constitute an effective supervisory approach and limits the authority's ability to systematically identify and address unauthorised activity.

4.2. Supervisors identifying, understanding and promoting DNFBP understanding of ML/TF risks

4.2.1. Identifying and maintaining an understanding of the ML/TF risks in the different sectors and types of DNFBPs and of individual DNFBPs over time

348. The FARS and OMPL, amongst other competent authorises, demonstrated to have better understanding of risk in their supervised sectors. Other supervisory authorities and SRBs demonstrated a more limited understanding of ML/TF risks within their supervised sectors. While all supervisory authorities and SRBs acknowledged the contents of the 2025 NRA, their levels of agreement with the findings varied considerably.

349. With the exception of the FARS and the OMLP, the other supervisory authorities or SRBs were unable to clearly articulate the ML/TF threats and vulnerabilities associated with the regulated DNFBP sectors under their supervision. Their understanding of risk did not align with the findings of the 2021 or 2025 NRA, which does identify inherent ML threats and vulnerabilities within several DNFBP activities. Instead, most authorities and SRBs primarily focused on risks arising in the unregulated market, rather than recognising or assessing threats and vulnerabilities within the regulated sectors.

350. Specifically, within the 2025 NRA the SBA acknowledges that criminals deliberately exploit the regulatory gap by using unregulated legal advisors instead of covered lawyers, and that the low volume of STRs arising from covered lawyers reflects a displacement of risk toward the unregulated legal advice sector. This issue had been previously raised within the 2021 NRA, however, no regulatory actions had been taken to address this risk. While this demonstrates awareness of risks outside the regulated activities, the SBA did not identify or articulate ML/TF risks inherent to the activities of covered lawyers, despite these being recognised in the NRA.

351. Similarly, the CNS highlighted that the biggest vulnerability arose from unregulated activities, namely from peer-to-peer real estate transactions which can be conducted without the involvement of a lawyer or notary to verify transaction details, demonstrating awareness of risks in unregulated channels. However, it did not recognise or articulate threats or vulnerabilities within the regulated sector itself, in line with the NRA. This suggests that while some DNFBP supervisors acknowledge displacement risks into unregulated areas, they tend to understate or dismiss threats and vulnerabilities within their own regulated sectors.

352. The FARS demonstrated a comprehensive knowledge of its sector and its activities, and in turn were able to recognise risks. The OMLP perceived a higher risk in OEs who have clients based or associated with higher risk countries, and the role of professional enablers potentially facilitating or being abused by criminals to conceal beneficial ownership and structure fictitious transactions.

353. Regarding TF, all supervisory authorities and SRBs appeared to equate Slovenia's TF threats and vulnerabilities with the absence of terrorism within Slovenia. Therefore, there has been no supervisory focus or targeted efforts to identify or address TF risks within their respective sectors. Nevertheless, it is not considered to be a serious deficiency given that the underlying TF risk is generally assessed as low.

354. Risk assessment activity across DNFBP supervisors appears to be confined to their participation in the preparation of the NRA. None of the supervisory authorities or SRBs have conducted independent sectoral risk assessments to identify or assess ML/TF risks within their sectors. This extends to the identification and assessment of evolving or emerging risks, which remains largely unaddressed.

355. For the completion of the NRA, supervisory authorities and SRBs that participated in the NRA working groups, issued questionnaires to all OEs within their respective sectors. These questionnaires

sought to collect information on sectoral characteristics and entity-specific risks. The scope and detail of information requested within the questionnaires varied across sectors. For instance, regarding accountants and tax advisors, information was requested on the services provided, types of customers, transactions involving high risk countries, risk scoring of the customer base, number and type of STRs, information on the exposure to virtual assets, the use of cash, the number of NPO customers, and sanctions related information. Similarly, the SBA requested information on the nature of the activities provided by covered lawyers, the risk profile of its customers, a breakdown on the type of CDD applied, number of PEPs, etc. In contrast, the questionnaires for the real estate and DPMS sectors were more limited, seeking only high level information on the number of customers, number and value of transactions, and confirmation that all policies and procedures had been implemented.

356. Overall, the reliability of those assessments are questionable given: (i) the insufficient scope and detail of collected data; (ii) an over-reliance on the information provided by OEs with no further verification conducted; and (iii) the low response rate (100% for covered lawyers and casinos, 53.5% for the real estate sector, 43% for accountants and tax advisors collectively, and 38.9% for dealers in precious metals, with no information for other DNFBP sectors). As a result, supervisory authorities and SRBs lack a clear and evidence-based understanding of ML/TF risks at a sectoral level.

357. With the exception of the FARS, other supervisory authorities and SRBs were unable to demonstrate instances where they had independently identified an ML/TF risk, threat, trend or typology. FARS noted an example of an emerging risk identified and addressed, relating to the proactive detection and blocking of illegal online providers. Moreover, there was no evidence of structured communication or coordination among competent authorities to share concerns or insights related to emerging risks, threats, or vulnerabilities.

358. None of the supervisory authorities or SRBs have established a formal risk methodology to assess and determine the risk profile of their OEs. Risk ratings assigned to OEs are based on subjective judgment of supervisory authorities and SRBs rather than on objective risk indicators. In addition, given the lack of reliable data on the number of operators within some sectors, such as accountants and tax advisors, the OMLP is unable to determine the overall risk profile of the sectors. This leads to a lack or an inadequate level of ML/TF risk perception of the supervised OEs. The CoN and SBA consider all registered notaries and covered lawyers respectively as a low risk. While the FARS does conduct a periodic risk assessment of its entities on the renewal of concessions it still classifies all casinos as a low ML/TF risk. This classification applied by all competent authorities does not align with the 2021 or 2025 NRA and does not take into consideration internationally recognised ML/TF risks commonly associated with those sectors.

359. The AT concludes that the overall effectiveness of supervisory authorities and SRBs in identifying and understanding ML/TF risks is weak. This limited understanding reflects the nature of supervisory activities, which hinders supervisors' ability to develop a comprehensive view of ML/TF risks within their respective sectors.

4.2.2. Promoting DNFBP understanding of ML/TF risks and AML/CFT obligations

360. All supervisory authorities and SRBs have taken some steps to promote ML/TF risk understanding across all DNFBP sectors though this is limited to the provision of generic guidelines and training. Nevertheless, the supervisors weak understanding of ML risks noted above, and basic level of performance demonstrated by the DNFBPs, is indicative of the necessity to substantially upscale the level of engagement on behalf of supervisory authorities and SRBs.

361. All DNFBPs were made aware of the NRA 2025 by means of publication, and some supervisors have disseminated the NRA directly to their respective sectors.

362. All supervisory authorities and SRBs have published sectoral guidelines on the application of AML/CFT measures, including ML/TF risk indicators. These guidelines have been updated to reflect amendments to the APMLTF-2 and were shared with all OEs. All OEs were aware of these guidelines and reported using them in practice.

363. The OMLP, in its capacity as the central authority for AML/CFT, the primary supervisory authority for tax advisors and accountants, and as secondary supervisor for all other DNFBP sectors, demonstrated the highest level of engagement in promoting and strengthening the understanding of ML/TF risks and AML/CFT obligations. The OMLP cooperates closely with all other DNFBP supervisors in drafting sectoral guidelines and delivery of training activities. The AT commends the OMLP's AML/CFT team for its commitment and efforts despite significant resource constraints. However, these efforts remain insufficient to address the broader shortcomings in understanding and awareness of ML/TF risks among DNFBP sectors and their supervisors.

364. In addition to the guidelines the supervisors organise regular trainings for their supervised sectors covering topics related to implementation of AML/CFT measures (amendments to APMLTF-2, EU regulatory framework, CDD measures, case examples, etc.). In particular, the OMLP organises annual trainings for all DNFBPs; the SBA conducts annual trainings for its members; the FARS and CoN organise biannual trainings for casinos and notaries respectively; the OMLP organised a specific training for tax advisors.

365. It is commendable that most of the authorities place strong emphasis on regular engagement with their supervised sectors. However, these efforts have not translated into a demonstrable understanding by DNFBPs of ML/TF risks and their AML/CFT obligations, as noted further in the analysis below. Further efforts by supervisory authorities and SRBs are therefore required to enhance the depth and practical application of DNFBPs' risk understanding, moving beyond high-level awareness towards a more targeted and risk-based approach.

4.3. DNFBP understanding of existing and evolving ML/TF risks

366. The limited understanding of ML/TF risks among DNFBPs, including by those sectors identified by Slovenia as posing a higher risk, constitutes a major obstacle to the overall effectiveness of Slovenia's AML/CFT system.

367. DNFBPs understanding of existing and evolving ML/TF risks was limited to the contents of the NRAs, specifically the 2025, that had been recently shared by supervisory authorities and SRBs. There was little awareness or acknowledgement of the 2021 NRA and its findings.

368. When discussing the ML/TF risks of the sectors, the OEs simply reiterated the conclusions of the 2025 NRA, without providing an in-depth and contextualised understanding of the specific threats and vulnerabilities relevant to their sectors or individual business activities.

369. The findings of the NRAs have not been assimilated or integrated into OEs risk assessments and internal controls. The majority of DNFBPs interviewed perceived their sector to be low risk, despite the threats and vulnerabilities identified by the NRAs. This reflects a discrepancy between the risks perceived by OEs and the reality of Slovenia's ML/TF risk landscape. This lack of awareness undermines the effective implementation of AML/CFT controls by OEs, such as the application of EDD or STR reporting.

370. OEs tend to underestimate their exposure to ML/TF, often reasoning that their business activities primarily involve local customers, that they encounter few suspicious transactions, and that the customer's use of the Slovenian banking system subjects them indirectly to the bank's full AML/CFT controls.

371. Covered lawyers and real estate entities did not recognise any ML/TF risk exposure within their sector or their own business activities. Covered lawyers focused primarily on the activities of unregulated legal advisors, which they viewed as posing a greater ML risk. Real estate entities asserted that the risk exposure only arises in peer-to-peer real estate transactions where an OE is not involved. This observation was also noted by the SBA and by the CNS, respectively.

372. DPMS could not articulate the threats and vulnerabilities of its sector or its activities.

373. Casinos demonstrated comparatively greater awareness and understanding of existing and evolving ML/TF risks. The casinos were well informed about the rationale behind FARS imposed AML/CFT obligations and showed awareness of relevant trends and typologies associated with games of chance activities. This understanding reflects the proactive and comprehensive supervisory efforts adopted by the FARS.

374. Tax advisors, accountants and auditors that are part of an international group displayed a more advanced understanding of their ML threats and risks, including knowledge of common trends or typologies. Whilst domestic OEs' understanding of risks was more limited.

375. All DNFBPs are obliged to complete an annual risk assessment. However, except for the entities which are part of an international group, such as tax advisors, accountants and auditors, these are largely carried out as an administrative exercise aligned with the Guidelines issued by the supervisory authorities and SRBs, and do not effectively consider their own individual risks. Furthermore, DNFBPs were unable to demonstrate the effectiveness of the assessments or how the results were used to amend or strengthen their internal controls. None of the sectors demonstrated forward-looking analysis to identify and assess emerging ML/TF risks arising from new activities, products, trends, technologies, etc.

376. With regard to TF, the understanding among DNFBPs was even more limited. The prevailing view, consistent with that of supervisory authorities and SRBs, was that TF does not happen in Slovenia. As a result, little attention has been devoted to these areas. The shortcomings identified within IO.1 regarding Slovenia's TF assessment, negatively contribute to the DNFBPs limited understanding and awareness of TF threats and vulnerabilities.

4.4. DNFBP understanding and compliance with AML/CFT obligations and mitigating measures

377. With the exception of Casinos and firms forming part of larger international groups, such as accountants, tax advisors, covered lawyers or auditors, the mitigating measures applied more generally by DNFBPs are confined to predetermined criteria set out in the supervisory authorities or SRBs guidelines, with no consideration given to their own individual risk exposures. The concept and practical application of a risk-based approach is non-existent.

378. Most DNFBPs across all sectors consider both their sector and their customer base to be low risk. This perception does not align with the findings of the 2021 or 2025 NRA and demonstrates a clear lack of understanding of ML/TF threats and vulnerabilities. These misconceptions undermine the effective implementation of AML/CFT controls by OEs, such as the application of EDD or STR reporting.

379. The absence of effective AML/CFT measures implemented by DNFBPs is particularly concerning, especially in sectors that Slovenia itself has identified as posing a higher ML/TF risk.

4.4.1 CDD, record-keeping, BO information, ongoing monitoring

380. The application of CDD, record-keeping, ongoing monitoring and BO identification varies across DNFBP sectors. With the exception of Casinos, DNFBPs advised that given the nature of their services the majority of their customers were considered one-off customers, an approach that aligns with common practice within DNFBP sectors. Consequently, where subsequent services are provided to the same customer, these are treated as a new business relationship, prompting the re-application of CDD each time. As a result, ongoing monitoring measures were largely not relevant to their business operations. Nevertheless, the repeated application of CDD ensures that customer identification and verification measures are refreshed for each engagement, which may contribute positively to maintaining up-to-date customer information.

381. *Real estate agents and notaries* generally collect only basic identification information. Where relevant, OEs referred to checks conducted through the Business Register and the BO register, however, they also reported challenges regarding data access and quality in the BO register. No other independent checks are conducted to assess the ML/TF risk of the customer or transaction. OEs do not examine the source of funds involved in transactions but rely solely on banks to carry out full CDD when processing payments.

382. *Covered lawyers* reported using onboarding questionnaires to collect initial information on customers, including details on the corporate structure, BO, and confirmation of the customer's PEP status. Following receipt of this information, OEs carry out due diligence using both public and non-public sources, such as court and business registries. Covered lawyers that are part of larger international groups also utilise third party CDD providers to perform additional checks and identify if there is any adverse information on the customer.

383. *Tax Advisors, Accountants and Auditors* that are part of larger international groups[20] demonstrated a higher level of understanding and compliance with its AML/CFT obligations, as opposed to the domestic ones. These OEs were able to articulate their CDD procedures, BO identification processes, the use of independent verification measures, etc., including the use of third party CDD providers to perform additional checks and identify if there is any adverse information on the customer.

384. OEs that only trade domestically or are not part of a larger international group, collect only basic identification data and in many cases lack comprehensive understanding of the need to identify and verify the BO of legal persons and legal arrangements. Similarly, the application of source of funds verification was largely non-existent.

385. *DPMSs* generally collect only basic identification data. The ones that operate internationally and partner with other parties, such as international banks, were able to explain the need and process of identifying BO information as part of its AML/CFT controls. No other independent checks are conducted to assess the potential ML/TF risk of the customer or transaction. Other DPMSs collect only basic identification information and do not carry out independent checks either.

386. *Casinos* demonstrated the highest level of understanding and application of AML/CFT mitigating measures, appropriate to the nature and risk of their business activities. The proactive supervision and the comprehensive requirements imposed by the FARS are clearly reflected in the sector's level of compliance

20. Accountants and auditors part of a larger international group comprise of 30% and 69% of the market, respectively. No similar data is available for the Tax Advisors.

and awareness. Casinos clearly articulated the CDD measures applied at the different stages, e.g., upon entering to Casino premises, and on pay out.

4.4.2 Enhanced or specific measures

387. All DNFBPs were aware of the legal obligations to apply EDD in higher risk scenarios. Nevertheless, the application of such measures in practice was not evident on all instances. Most of the DNFBPs demonstrated a limited understanding of the specific measures required for these cases, including those involving PEPs and high-risk countries, and could not articulate a clear distinction between the different categories of due diligence measures.

388. All DNFBPs demonstrated to be aware of the obligation to identify whether the customer or its BOs are PEP and the need to apply EDD measures to these individuals. Nevertheless, most DNFBPs across all sectors did not demonstrate a clear understanding of the specific measures that should be applied to PEPs. In particular, they did not always recognise the need to carry out source of wealth checks, often relied on banks for verification of source of funds, and some were unaware of the need to obtain senior management approval for these business relationships. This could be because of inadequate CDD or weak BO identification controls, or a low exposure to PEPs within the DNFBP sectors. The limited supervisory activity carried out by supervisory authorities and SRBs are not conducive to identify shortcomings in this area.

389. Accountants, tax advisors, and auditors that are part of larger international groups, demonstrated a stronger understanding of PEP requirements. This is primarily attributed to the implementation of group wide comprehensive CDD procedures, and structured access to reliable third-party databases that facilitate screening and verification.

390. All DNFBPs demonstrated the knowledge of the high-risk jurisdictions list issued and regularly updated by the OMLP. Understanding of obligations related to higher risk countries varied considerably across DNFBPs. Most OEs were able to articulate the legal requirement to apply EDD where a customer or transaction is linked to a higher risk country. However, with the exception of covered lawyers, tax advisors, accountants and auditors that form part of larger international groups, other DNFBPs across the other sectors or trading primarily domestically, were not able to describe the specific enhanced measures they would apply in practice and would refer to the guidance provided by their relevant supervisor if the case for EDD arose. When questioned regarding customers or transactions involving a neighbouring country that was until recently included within the FATF's list of high-risk jurisdictions, the application of EDD, in accordance with Slovenia's legal provisions under the APMLTF-2, varied considerably between sectors. Covered lawyers advised if a customer transaction involved a property outside of Slovenia, they would partner with a legal advisor in the relevant jurisdiction. The DPMS sector provided an example where they were transacting with a higher risk country, and it recognised the need to provide enhanced information to the Bank to conclude the business transaction.

4.4.3 AML/CFT reporting obligations, tipping off

391. With the exception of Casinos, DNFBPs do not understand or apply their AML/CFT reporting obligations effectively. Reporting of STRs by other sectors did not reflect adequately on the ML/TF risk within the relevant sectors (see Table 6.1 in Chapter 6).

392. Contrary to the FATF Standards and to the legal provisions within the APMLTF-2, the majority of OEs advised that in cases of a suspicious customers or transactions, they prefer to reject the customer rather than submit an STR to the OMLP. The few examples presented by OEs related primarily to cases of potential

tax evasion, and where not reported to the OMLP. In one example, the OE advised that it had identified a customer who appeared to be structuring a transaction to avoid tax obligations, however when being asked why it was not reported the OE explained that it considered it was a simple mistake and that it had informed the customer about the possible consequences with the tax authorities.

393. OEs also reiterated their reliance on banks' CDD measures, specifically regarding the verification of source of funds. Therefore, the significant shortcomings in the application of AML/CFT measures, combined with the over-reliance on bank AML/CFT measures, contribute to the low number of STRs.

394. No STRs have been submitted by DNFBPs in relation to TF. While the AT acknowledges Slovenia's low TF risk and it has not identified a specific unreported case that could raise immediate concerns, the lack of STRs may be considered reflective of the low level of TF risk understanding among DNFBPs.

395. Most OEs were aware that STRs must be reported to the OMLP and had access to the reporting form published by the OMLP. However, many also advised that such reports would be simultaneously submitted to their supervisory authority or SRB, suggesting confusion regarding appropriate reporting channels. As a result, OEs generally opted to report to both authorities to ensure a correct submission. Furthermore, none of the OEs provided information on the process to follow if consent from the OMLP is required prior to proceeding with a transaction.

396. With respect to tipping off, the majority of OEs were able to articulate the legal prohibition but were unable to elaborate on what controls were in place or would be implemented to prevent inadvertent disclosure. Most OEs advised they would refer the matter to their designated AML/CFT compliance officer.

397. Neither the supervisory authorities, SRBs nor the OMLP (in its capacity as financial intelligence unit) have undertaken targeted training or outreach to address the deficiencies identified, particularly the lack of STR reporting.

4.4.4 Internal controls, procedures and audit to ensure compliance

398. Few OEs have established formal policies and procedures tailored to their own specific risk profiles. Updates to these frameworks are infrequent, and training remains inadequate.

399. Among the sectors demonstrating stronger compliance, Casinos maintain internal procedures that demonstrate compliance with all AML/CFT obligations. Similarly, accountants, tax advisors, auditors, and covered lawyers which are part of larger international groups were able to demonstrate the implementation of effective and documented internal controls, including the application of a risk-based approach to its activities.

400. Other DNFBPs view internal controls as an administrative requirement, often treating the supervisory authorities or SRBs guidelines as a checklist rather than understanding the need to integrate effective AML/CFT measures into their operational processes.

401. Many OEs met during the onsite did not provide regular in-depth AML/CFT training to their staff, which hinders their understanding and level of AML/CFT compliance. Training efforts appear largely confined to attendance by AML/CFT compliance officers in the annual sessions organised by the OMLP, after which they are expected to train their staff. The AT considers this approach insufficient given the observed shortcomings in DNFBPs understanding of AML/CFT requirements and risks.

402. Accountants, tax advisors, and auditors that are part of a larger international group demonstrated comprehensive policies concerning the application of audit controls to their AML/CFT controls ranging from the use of external providers and internal audit functions. Casinos and real estate entities also

acknowledged internal audit measures to some extent. None the other sectors provided comprehensive information on this matter.

4.4.5 Legal or regulatory impediments to implementing AML/CFT obligations and mitigating measures

403. As noted within R1.7 and IO1, there are limitations in the scope of Slovenia's AML/CFT framework for DNFBPs, given it is unclear if legal advisors are able to provide FATF defined activities in R22.1(d). Regarding the other DNFBPs that fall within the scope of the APMLTF-2, the AT did not identify any major obstacles to the implementation of AML/CFT obligations and mitigating measures.

4.5. Supervisors risk-based monitoring or supervising compliance by DNFBPs

404. All regulated sectors have a designated supervisory authority or SRB that holds responsibility to supervise compliance with APMLTF-2. In addition to the designated primary supervisory authority or SRB identified for each sector, the OMLP acts as the secondary supervisor for all DNFBPs.

405. For most sectors, supervisory activities are often limited to formal reviews of documents rather than a comprehensive assessment of the practical implementation or effectiveness of the AML/CFT measures implemented by OEs. None of the supervisory authorities or SRBs demonstrated the application of a risk-based approach to supervision, whereby greater focus is expected to be placed on higher risk sectors and higher risk OEs. This could be reflective of the limited risk understanding of the sectors and OE risk profiles.

406. The absence of comprehensive information to identify the number and types of persons actively operating as real estate entities, tax advisors, accountants, and DPMSs, and a lack of information on legal professionals that are not registered with the SBA, renders effective supervision of these sectors impossible. This is particularly concerning because some of these sectors are identified within the NRA as posing a higher risk of ML.

407. *Real estate entities and DPMSs* – The MIRS conducts the AML/CFT supervision of real estate entities (business entities and registered real estate agents) and DPMSs.

408. The MIRS advised that it lacks sufficient human resources to implement an effective and sustainable supervisory framework. In addition to the supervision of real estate and DPMS sectors, the MIRS is responsible for several other financial and non-financial sectors. The AML/CFT team comprises of 8 inspectors though they are not dedicated exclusively to AML/CFT functions.

409. Whilst the Ministry of Solidarity-Based Future maintains a register of real estate agents, and the Metrology Institute registers DPMS (except for traders in precious stones and raw metals), the MIRS does not have access to reliable and up to date information on the number of Real Estate entities or DPMS' actively operating within these sectors. It relies on the business register. However, MIRS advised that it is not a reliable source either as many persons register multiple activities irrespective of whether they are actually performed. The MIRS has identified numerous cases where the person has confirmed that they are in fact not carrying out these activities. In these cases, the MIRS does not verify that the person is actually not conducting regulated activities.

410. In 2024, the MIRS adopted a pro-active supervisory approach, and towards the end of the year, issued questionnaires to all 2 777 OEs registered with the Business Registry for real estate and DPMS activities. The questionnaire requested confirmation if the person was undertaking regulated activities and had complied with the various AML/CFT obligations and collected high level information on the number of customers.

411. The response rate from the real estate sector was 53.5% with at least 11% of responses incomplete. The response rate from DPMSs was even lower, at 38.9%, with at least 3% of responses incomplete. The MIRS does not have the legal powers, nor has it implemented practical procedures to follow up with non-respondents, and no supervisory actions were taken against entities that failed to respond. The absence of complete and reliable information from OEs undermines the implementation of effective supervisory measures.

Table 4.2. Risk Rating (only for those entities that responded to the questionnaires)

	Low Risk	Medium Risk	High Risk
Real estate entities	60%	39%	1%
DPMS	71%	28%	1%

412. MIRS inspection procedures require that OEs provide inspectors with all relevant AML/CFT documents during the inspection visit that typically lasts half a day and includes the review of 3-5 client files to verify the application of the OEs policies and procedures. On completion of the inspection, the MIRS completes an inspection report detailing the actions taken by inspectors and the findings. Client files are randomly selected ranging in characteristics; however, inspections are not risk based or target the specific risks of the OE e.g. focus on higher risk customers or higher risk transactions. Inspections of such limited duration are not sufficient to allow for an in-depth and comprehensive assessment of an OE's internal controls or the effective implementation of AML/CFT measures in practice. Moreso considering the limitations in the supervisory framework for real estate sectors and DPMS, and that these are considered as posing a higher risk in accordance with Slovenia's NRAs. Furthermore, the MIRS does not risk assess the OE after an inspection, nor does it place it in a periodic supervisory programme. As a result, the inspection process lacks depth and continuity, limiting its effectiveness in identifying risks or the promotion of sustained compliance by OEs.

413. The MIRS does not apply a risk-based methodology to determine its supervisory activities. The annual supervisory plan is determined based on the availability of human resources rather than the sectors or individual OE risks. Between 2020-2024 the MIRS conducted a total of 183 inspections in the real estate sector, representing 13% of it. (See Table 4.3). No inspections have been carried out on DPMSs.

414. *Covered Lawyers* – The SBA is responsible for the AML/CFT supervision of covered lawyers. As of the end of 2024, there were 1 913 registered covered lawyers.

415. The SBA's offsite supervisory efforts are comparatively more developed. At the end of 2024 the SBA issued questionnaires to all covered lawyers, requesting confirmation if the person was undertaking regulated activities, the nature of activities provided, the type of controls implemented, information of the risk profile of its customers, etc. The SBA carried out a comprehensive analysis of the result. However, given the lack of risk categorisation it results in an inadequate application of supervisory framework.

416. The SBA also lacks a methodology to determine its risk-based supervisory activities. The SBA noted that it is comprised by covered lawyers that carry out this function on a voluntary basis, with 5 Commission Members and only one dedicated resource to fulfil its supervisory obligations. As a result, supervision is largely limited to offsite reviews through the submission of annual questionnaires to verify or assess covered lawyers AML/CFT controls.

417. The SBA has established documented procedures for its supervisory activities, including inspections. Inspections are carried out by the dedicated professional and one Commission Member. The inspection is concluded in three parts; 1) request for review of general AML/CFT documents, including a written risk assessment of customers, control measures for risk management, CDD measures, training, list of indicators

and thresholds for customers and transactions; 2) review of selected clients or transactions which includes a review of the 5 largest transactions; and 3) a sample review of transactions over €15,000 and review of at least one PEP business relationships (if relevant). On completion of the inspection, the SBA completes an inspection report detailing the actions taken by inspectors and the findings.

418. *Tax Advisors and Accountants* – The OMLP is the designated supervisory authority for tax advisors and accountants.

419. Due to the absence of registration or licensing regimes for tax advisors and accountants, the OMLP does not have reliable and up to date information on the number of OEs operating within these sectors. The OMLP relies on the business register to identify persons that have registered as providing these activities, though it acknowledges that this is not a reliable and accurate source as many persons register multiple activities regardless of whether they are actually performed. As a result, the OMLP also monitors how entities or individuals advertise their services through public sites and consults with AJPES regarding tax returns, that could identify if any entities or individuals carrying our regulated activities. The OMLP has identified a number of cases where the person confirmed that it did not conduct these activities. In these cases the OMLP does not verify that the person is in fact not conducting regulated activities.

420. The OMLP does not carry out any offsite supervision and relies solely on onsite inspections for its supervisory activities.

421. Furthermore, the OMLP does not apply a risk-based methodology to determine its supervisory activities. Its annual supervisory plan is driven by the human resources available, and within the resources available it determines the OEs selected based on its perceived risk profile (although this has not been provided to the AT to assess its effectiveness). The OMLP AML/CFT team is comprised of 6 inspectors and between 2020-2024, the OMLP conducted a total of 886 inspections on accountants and tax advisors, (see Table 4.3).

422. Following each inspection, the OMLP completes a detailed inspection report that outlines the actions of the inspector. Inspections typically last half a day, which the AT considers insufficient to conduct an in-depth exhaustive review of all policies and procedures and verify the effective application of AML/CFT controls. Furthermore, it does not risk assess the OE after an inspection, nor does it place it in a structured supervisory programme.

423. Given the large number of OEs under its supervision, its additional role as secondary supervisor of all other DNFBP sectors, and its broader mandate as Slovenia's central authority for AML/CFT, the AT commends the team for maintaining this level of supervision despite being significantly under-resourced. However, when considered against the available staffing levels, the volume of inspections raises concerns as to whether these can be conducted with sufficient depth and effectiveness.

424. *Casinos* – The FARS is the designated supervisory authority for Casinos. As of the end of 2024, there were 35 registered operators providing games of chance activities.

425. The FARS has the most developed and operationally effective supervisory framework among the DNFBP supervisors, and demonstrated active, ongoing supervision of the Casino sector. Supervision is conducted through a combination of 1) transactional analysis – all Casinos have their transactions directly connected to the FARS monitoring system, 2) offsite supervision such as periodic questionnaires, and 3) inspections which cover the full scope of AML/CFT obligations or target specific areas. OEs interviewed also acknowledged the high frequency and thoroughness of FARS inspections.

426. The FARS has developed comprehensive internal procedures for the implementation and conduct of supervisory activities.

427. *Notaries* – Notaries are supervised for AML/CFT purposes by the CNS. As of the end of 2024, there were 86 registered notaries.

428. The CNS similarly lacks a risk-based approach to determine its supervisory activities. Its annual supervisory plan is determined solely on available human resources, with a focus to cover at least 15% of practicing notaries and does not consider the sectors or individual OE risks. Between 2020-2024, the CNS conducted a total of 33 inspections, covering 38% of the sector (see Table 4.3). Notaries are advised of an inspection visit 2 days in advance. All documents are obtained and reviewed during the onsite visit, including the review of 3-5 client files to verify the application of the OEs AML/CFT controls. Inspections typically last half a day, which the AT considers is insufficient to complete an in-depth exhaustive review of all policies and procedures and verify the effective application of AML/CFT controls.

429. The CNS does not have documented internal procedures for its supervisory activities but instead relies on the general provisions within Slovenian legislation, namely the Notary and Inspections Acts. While the Acts outlines the powers available to inspectors and provides a general framework for inspection procedures, it remains high level and lacks detail. This poses a risk of inconsistent practices among inspectors and does not represent a sound or effective approach to AML/CFT risk-based supervision.

430. *Auditors* – The APOA is the designated supervisory authority for auditors. As of the end of 2024, there were 167 registered auditors and 49 audit firms.

431. The APOA has not adopted a dedicated AML/CFT supervisory framework and lacks an AML/CFT specific risk assessment methodology. Instead, AML/CFT compliance is reviewed as an ancillary component within the broader audit and tax supervision framework. Inspections are conducted only when a regular audit or tax review is due, rather than on the basis of ML/TF risk. Nonetheless, the APOA demonstrated a satisfactory level of supervisory activity, conducting a total of 52 inspections between 2020-2024. This means that all audit firms have been subject to an onsite inspection during the assessed period.

Table 4.3. Inspections undertaken

	2020	2021	2022	2023	2024
Real estate	32	1	95	1	53
Covered Lawyers	0	0	4	3	10
Accountants/tax advisors	163	133	255	186	149
DPMS	0	0	0	0	0
Casinos	74	38	87	70	87
Notaries	2	6	5	12	8
Auditors	10	9	12	13	8

4.6. Impact of monitoring, supervision, outreach, remedial actions and effective, proportionate and dissuasive sanctions on DNFBP compliance

432. Supervisory authorities and SRBs have a range of remedial measures and sanctions provisions at their disposal. However, except for Casino, Accountant and Real Estate sectors, there were no enforcement measures applied since supervisors advised that no AML/CFT infringements were detected. Nonetheless, in case of AML/CFT infringements, supervisory authorities and SRBs advised to favour the application of remedial measures and warning notices, with little to no consideration taken of other types of sanctions such as penalty fees or withdrawal of individuals in management functions. None of the other supervisory authorities or SRBs have a documented sanctioning framework.

433. The shortcomings noted above regarding the ineffectiveness of the supervisory efforts by supervisory authorities and SRBs, is the primary factor of the lack of enforcement actions.

Table 4.4. Summary of sanctions imposed 2020-2024

	No. of inspections having identified AML/CFT infringements	Remedial measures	No. of written warnings	Fines
Real estate	49	23	46	0
Covered Lawyers	0	0	10	0
Accountants/Tax Advisors	122	122	9	6 EUR 10,310
DPMS	0	0	0	0
Casinos	591	3	4	4 EUR 12,894
Notaries	0	0	0	0
Auditors	19	19	0	0

434. Even within these three sectors where sanctions measures have been applied, they are still insufficient.

435. *Real Estate entities* – MIRS favours the issuance of written warnings and places the obligation on real estate entities to rectify the shortcomings identified. Following a remediation notice, MIRS advised that it carries out a follow up visit to verify that shortcomings have been adequately addressed. The follow up visit follows the same steps and process as a standard inspection visit e.g. documents are required prior to the visit for an initial desk-based review, and an inspection report noting the outcome of the inspections is completed and kept on record.

436. *Casinos* – The FARS is the most developed DNFBP supervisory authority. However, the number of sanctions imposed cannot be considered as effective, proportionate or dissuasive. From 591 inspections where deficiencies were identified (for which Slovenia has not clarified the reason for the high numbers and nature of infringements), only three entities were imposed remedial action (0.5%), only 4 were issued a written warning (0.7%), and only 4 were imposed a monetary fine (0.7%). The monetary fine on average per entity amounts to EUR 3,223 which is considered quite insignificant. The FARS considers that the low level of enforcement action is reflective of the comprehensive supervisory measures. However, the low volume of enforcement actions in comparison to the number of inspections identifying shortcomings (1.9%) is indicative of a lenient sanctioning approach.

437. *Accountants and auditors* – The OMLP and APOA favour the application of remedial measures and places the obligation on OEs to rectify the shortcomings identified. However, there is no supervisory follow up to verify that the findings have been adequately addressed. Only 6 accountants were imposed a monetary fine (4.9%), whilst no auditors were imposed any other sanctions measures.

438. The OMLP has established and documented procedures for the application of sanctions regarding the sectors it acts as primary supervisor i.e. tax advisors and accountants. The OMLP's procedures defines that a warning is always issued as a first step instead of a sanction where the offence is of minor importance and where the inspector considers that a warning is a sufficient measure. The decision on whether to issue a warning or a fine, and the fine amount, falls with the inspector who carried out the inspection. However, the written procedures are not detailed enough to determine the methodology to sanctioning decision nor to ensure consistency in the application of these measures across inspectors.

439. Overall, the supervisory authorities and SRBs apply lenient sanctioning policies, and the lack of enforcement seriously undermines Slovenia's effectiveness to mitigate ML/TF risks or address AML/CFT compliance concerns.

440. With the exception of published guidelines, and as noted in Chapter 4.3, the OMLP is the only supervisory authority to carry out outreach to raise OEs awareness of their obligations. None of the supervisory authorities or SRBs were able to articulate or demonstrate how their supervisory actions positively impacted compliance by DNFBPs. This is largely due to the ineffective supervisory frameworks, lack of knowledge of the OEs, and lack of records maintained.

441. The AT observed that the DNFBPs awareness and understanding remains insufficient, as most do not fully understand the importance of implementing effective AML/CFT measures or are not fully familiar with their obligations. The lack of educational measures or enforcement action undermines efforts to address these significant concerns.

Chapter 5. Transparency and Beneficial Ownership

The relevant Immediate Outcome considered and assessed in this chapter is IO.5. The Recommendations relevant for the assessment of effectiveness under this chapter are R.24-25 and elements of R.1, 10, 22, 37 and 40.[21]

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Slovenia's NRA provides some insights into how legal persons (LP) can be abused for ML/TF as key aspects like beneficial ownership (BO) are not considered and trends like legal persons (LPs) being struck off upon being investigated are not examined. Other aspects like the use of complex structures, strawmen and of shell and/or shelf companies, are mentioned, and a number of authorities understand these phenomena as they either encounter them or, in case of tax authorities, analyse and make use of related indicia to identify possible actionable cases. However, authorities have expressed differing views on the frequency with which these present themselves. This is also due to there being no generally shared and data-driven understanding of what are the actual ML/TF risks presented by LPs to Slovenia.

b) A series of measures are in place to limit the possible misuse of LPs registered through the Court Registries (CR), though these are not fully comprehensive particularly with respect to sanctions screening. All LPs have to be registered, and basic information is publicly accessible through the SBR. The information contained therein is deemed to be adequate. There are however limited checks to ensure that changes are effectively communicated by the LPs in a timely manner.

c) BO information is accessible through obliged entities (OEs), especially banks. Over 95% of LPs hold an account with a Slovenian bank, though this is more limited for branches of foreign LPs. OEs have demonstrated at least a basic understanding of the notion of BO, with FIs, especially banks, having a more in-depth and articulated knowledge of BO compared to other OEs from less material sectors. However, the limited supervisory activity by AML/CFT supervisors does not ensure that BO information held by all OEs, especially within the DNFBP sector, is accurate and updated in a timely manner.

d) The adequacy of BO information is ensured through Slovenia's system of publicly accessible registers, which also includes a Register of Beneficial Ownership (RBO). Authorities undertook a series of actions to ensure that it is fully populated. Foreign LPs present in Slovenia through a branch are also included in the RBO. Authorities and OEs have equal access thereto.

e) As acknowledged by authorities and OEs, the BO information available through the RBO may not be fully accurate and up-to-date, potential gaps being attributable to the lack of proper controls and verification checks. While the main onus is placed on OEs to check whether LPs submit

21 The availability of accurate and up-to-date basic and beneficial ownership information is also assessed by the OECD Global Forum on Transparency and Exchange of Information for Tax Purposes. In some cases, the findings may differ due to differences in the FATF and Global Forum's respective methodologies, objectives and scope of the standards.

information to the RBO and keep it updated, some OEs do not report discrepancies as required of them. These checks by OEs are supplemented through some supervisory activities and tax inspections, however supervisory oversight in the case of DNFBPs is quite restricted while insufficient resources limit the supervisory activities of the OMLP. Thus, the RBO data related to only a limited part of the LPs' population has been verified to ensure LPs have properly complied with their BO disclosure obligations.

f) Sanctions against LPs do not seem to be proportionate, effective and dissuasive, with only a restricted number of warnings and/or fines having been imposed. For a considerable period of time, authorities focused more on addressing failures related to BO information through remediation and have only recently adopted a more robust approach in this regard.

Key Recommended Actions (KRA)

a) Slovenia should assess the ML/TF risks presented by domestic and foreign LPs as well as legal arrangements, using widest range of datasets and information and analysing aspects like strawmen, the phenomenon of struck-off companies and the use of shelf and shell companies. Slovenia should take commensurate measures to address and mitigate any identified risks.

b) To limit the potential misuse of LPs for ML/TF purposes, Slovenia should strengthen the existing mechanisms and introduce new mechanisms where necessary ensuring: (i) timely submission of accurate BO information upon registration of new LPs; (ii) timely detection and registration of changes to basic and BO information, and (iii) supervision of the accuracy and timely update of information by LPs.

Other Recommended Actions

a) Supervisory authorities should make a more systematic use of the data available to them, especially the SBR and the RBO, to identify those LPs that present a higher ML/TF risk and inform the supervisory approach of authorities in this regard. Authorities should exchange information and coordinate their efforts to ensure the greatest coverage possible.

b) AJPES and AML/CFT supervisory authorities should increase further their outreach to both OEs and LPs with regards to their obligations related to basic and BO information in an effort to ensure better reporting of information to the SBR and RBO and improve upon the discrepancy reporting mechanism. Better direction should be provided to OEs as to which discrepancies are not to be reported.

c) Slovenia should ensure that authorities make greater use of pecuniary and non-pecuniary penalties for failures related to basic and BO information disclosure obligations, including by addressing any possible limitations arising from the use of the misdemeanour procedure under the Minor Offences Act. Consideration should also be given to whether the pecuniary and non-pecuniary penalties available to authorities need to be increased, and a methodology for their imposition be introduced, in order to ensure that sanctions are proportionate, effective and dissuasive, and reflective of the seriousness of any detected breaches.

Overall Conclusions on IO.5

Slovenia has taken some steps to understand and assess the ML/TF risks presented by LPs, be they domestic or foreign. However, this has been limited through the absence of proper consideration of aspects like the presence of the strawmen, shelf and shell companies, while no attempt has been made to understand phenomena like the number of limited liability companies (LLC) being liquidated on an annual basis, especially once these are object of investigation by LEAs. Reflected in their day-to-day activities, some authorities have a deeper understanding of how LPs can be abused in specific areas, but this cannot replace the need for a commonly shared understanding of ML/TF risks in this area. Given the inability to establish trusts and similar arrangements under Slovenian law coupled with the country's limited exposure to this phenomenon, it is a less pressing issue that the possible ML/TF risks associated with legal arrangements have not been considered in the 2025 NRA.

Some positive steps to prevent the abuse and increase the transparency of LPs and legal arrangements have been taken, with the SBR and the RBO holding significant basic and BO information, albeit the RBO is not yet fully populated. Additional safeguards include a degree of checks carried out on the founders of most LPs and the prohibition of nominee directors and shareholders.

This notwithstanding, there are still shortcomings to ensure that the basic and BO information accessible by the authorities, is accurate and current. Operationally, it has been shown that there are issues with the quality of the data in the RBO. While some supervisory and enforcement actions are being taken to identify and address failures related to basic or BO information, there is considerable dependence on the ability of OEs, especially banks, to detect issues with the reported information, which weakens the effective implementation of a multi-pronged approach. Sanctions against LPs do not seem to be proportionate, effective and dissuasive.

Slovenia is rated as having a moderate level of effectiveness for IO.5.

442. As of end December 2024, there were a total of 109,420 LPs registered in Slovenia, the greater part being companies established in terms of the Companies Law. LLC accounts for 70% of all registered LPs.

Table 5.1: Types of Legal Persons registered in Slovenia

Type of Legal Person	Number
Unlimited company (d.n.o.)	280
Limited partnership (k.d.)	160
Limited liability company (d.o.o.)	76 260
Joint-stock company (d.d.)	373
Economic interest grouping, GIZ	117
Limited liability cooperative (z.o.o.)	335
No-liability cooperative (z.b.o.)	111
Main office of a foreign business entity	395
Institute	4 110
Political party	86
Trade Union	2 715
Religious community and similar religious organizations	1 090
Association	23 013

Foundation	292
Total	**109 337**

443. Slovenia is not a major financial centre, with the registered companies averaging to approximately 3 600 companies a year over the assessment period. The greater part of these would be LLCs. The number of companies that is being struck off the SBR each year averages to 2 900 companies. These trends have been constant for the assessment period.

Table 5.2 – Registration and Termination of Companies (2020 – 2024)

	New Registrations	Termination
2020	3 333	2 849
2021	3 668	3 522
2022	3 786	2 802
2023	3 761	2 833
2024	3 607	2 494

444. LPs registered in Slovenia are not usually characterised by complex ownership and control structures. The percentage of companies where legal ownership is exercised through other LPs and/or arrangements is quite contained, the highest being an average of 13% in the case of LLCs. On the other hand, foundations present a higher percentage at around an average of 30% over the assessment period.

445. Slovenia has had a RBO in place since December 2017 and a requirement for branches of LPs present in Slovenia to disclose BO information thereto. There are currently 81 191 LPs in the RBO, which constitutes roughly 74% of the entire LPs population, and 115 536 individuals registered thereon as a BO. 86% of the registered BOs are Slovenian nationals or residents. The shortfall between the entire LP population and the population on the RBO is due in part to JSCs and public LPs not being required to be included in the RBO but also in part due to most single-member LLCs having to still be registered on the RBO, The greatest concentration of foreign BOs is associated with LLCs, with 14% of all registered BOs being foreign nationals. Foreign BOs are mostly resident within the Balkans or Central Europe with whom Slovenia has close economic ties.

446. Legal arrangements are not recognised under the laws of Slovenia.

5.1. Identifying, assessing and understanding ML/TF risks of legal persons and arrangements

Domestic Legal Persons

447. Slovenia has concluded its 2025 NRA. While the 2025 NRA does not analyse LPs, it does contain some insights into whether LPs are being abused for ML or FT purposes. Data provided by LEAs and included in the 2025 NRA on financial investigations show that these investigations often involve LPs and they are also at times referred to the State Prosecutor for further investigation. Indeed, Slovenia managed to obtain a conviction of an LP in 2021. A number of investigations into LPs and possible prosecution by the State Prosecutor are often stalled because the LP goes into liquidation due to bankruptcy.

448. However, these indications were somewhat limited as the 2025 NRA failed to analyse further the profile of LPs used in criminal activities – no consideration was given as to the main legal form that is encountered in the context of criminal activity, and neither was any attention given as to whether the BOs thereof were Slovenian or foreign residents. Equally, no consideration was given as to their ownership and

control structure, whether they had any active trading activity on-going, and within the context of which criminal activity, or at what stage of the criminal activity, these LPs were being used.

449. The 2025 NRA also identifies possible vulnerabilities associated with LPs, including complex ownership structures intended to obfuscate the BO(s), the possible use of LPs as shell and shelf companies as well as the presence of nominee directors/shareholders. However, it is not clear whether these are actual characteristics of LPs registered in Slovenia or just a general description of vulnerabilities often associated with LPs when it comes to ML, as authorities did not always concur to what degree these phenomena present themselves. On the other hand, data provided to the AT suggests that complex ownership structures may not be that common.

450. This absence of in-depth analysis and consideration of key data sets regarding LPs is pervasive throughout the 2025 NRA as no use or analysis was made of data that could otherwise be provided by AJPES, including whether trends to liquidate significant number of LPs is symptomatic of something more. In addition, the 2025 NRA does not provide any analysis of the effectiveness of the RBO, of the SBR and of supervisory activities to ensure that LPs and OEs comply with their basic and BO disclosure obligations.

451. As regards any possible TF risks, the 2025 NRA does make passing reference to possible instances where LPs registered in Slovenia may have been involved in TF cases. However, the manner in which the LP may have been abused and whether it merits the undertaking of any mitigating measures was not analysed. This notwithstanding, the prevalent consideration by Slovenia is that the overall risk of TF is low throughout all sectors and areas.

452. The 2025 NRA did not identify any particular typology as to how LPs are being abused for ML/TF, nor is it currently supplemented by any sectoral risk assessment or other analysis focused on LPs. One exception is a series of analyses prepared by FARS between 2019-2023 on the basis of 2018 data, which did conclude that shell and shelf companies, together with strawmen were all phenomena that could be noticed from the data analysed, and there was an established trend to use LLCs within international VAT carousel schemes. Indeed, FARS use indicia like the lack of economic activity by LLCs, LLCs registered at the same address or having the same legal representative to identify LLCs that are more likely to be abused for tax evasion or fraud. In addition, the OMLP's Annual Report does highlight ML/TF typologies associated with LPs, including the use of shell companies and the use of bank accounts held by LPs to channel possible proceeds of crime.

453. OMLP, FARS and LEAs referred to a number of typologies associated with LPs registered in Slovenia, where they would either be used directly in the commission of an offence or used to launder the proceeds of crime. Examples include the use of companies in VAT carousel schemes, in online fraud schemes, or the acquisition of immovable property through shell companies or companies fronted by strawmen financed with proceeds of crime. Another common typology involves companies beneficially owned by individuals of particular nationalities. In the latter case, the LP would be incorporated to circumvent local restrictions on the acquisition of immovable property or to channel funds into Slovenia for eventual withdrawal. However, AML/CFT supervisory authorities were of the view that these were no longer occurring as they were no longer detecting them through their activities.

454. While authorities all have a general understanding of the ML/TF risks generally associated with LPs, how these may manifest themselves and of possible trends and typologies, the depth of their understanding varies from one authority to another, underlying the absence of a shared understanding of the risks, threats and vulnerabilities presented by LPs in Slovenia. The absence of a data-driven exercise specifically focused on LPs is a further limitation in this regard.

Foreign Legal Persons

455. The 2025 NRA did not draw any specific distinction between domestic and foreign LPs. It did consider the exposure of the FI sector to non-resident customers, including LPs, but the data was not sufficiently granular to come to any conclusion on the matter. In addition, most competent authorities did not provide any particular insights as to how foreign LPs can pose an ML/TF risk to the Slovenian financial system. The SPO did however refer to how companies from a third country within the Balkans region were used as part of criminal schemes targeting Slovenia or forming part of wider schemes and involving companies in Slovenia as well.

Legal Arrangements

456. Legal arrangements were not considered in Slovenia's 2025 NRA. Trusts and similar legal arrangements cannot be established under Slovenian law and it does not seem that foreign legal arrangements are active in Slovenia. Competent authorities and private sector representatives met during the on-site visit reported having encountered trusts or legal arrangements only rarely within corporate ownership structures. However, this does not eliminate any ML/TF risks that may arise from having Slovenian residents acting as trustees for trusts or similar legal arrangements which are active outside of Slovenia. The indications are therefore that this is not a material area for Slovenia, though it cannot be definitely concluded that this is the case.

5.2. Mitigating measures preventing misuse of legal persons and arrangements

457. Slovenia has put in place a series of measures to mitigate the misuse of LPs. All LPs that can be set up in Slovenia, including branches of foreign LPs, have to be registered to be able to operate within Slovenia. Though the registration process differs from one LP to another, all LPs must ultimately be entered into a register. The companies and other LPs, who are registered into the Court Register (CR), must submit to relevant data and documents, including their statutory documents, with their registration application. Applications for registration can be made either through a notary or through SPOT, a government service which can assist anyone interested in establishing an LP in Slovenia. The different authorities responsible for registration of LPs have to establish whether the requirements set out in law for the registration of a particular kind of LP are met. The registers then feed into a centralised SBR administered and managed by AJPES.

458. Checks on the good standing of the founder of an LP are carried out in the case of companies and other LPs that are registered through the CR. These include all LPs, with exception of foundations and associations. These checks include whether the founder or the shareholder has been subject to a final conviction for a criminal offence against the economy, against employment relations and social security, against legal transactions, against property, against the environment, spatial planning and natural resources, and is registered in the criminal record of the MoJ. It also includes whether, the founder or the shareholder has been publicly listed in the last 12 months in one of the public lists indicating tax-related failures linked to the individual himself or a company in which he was directly or indirectly involved as a founder or a shareholder with more than 25% of the share capital. The failures in question include failure to submit tax declarations, failure to pay tax due, or termination of one's VAT registration. Checks also include whether the person has been fined in the previous 3-year period in a final decision issued by the Labour Inspectorate of the Republic of Slovenia or FARS for an offence relating to payment for work or an offence relating to illegal employment. Checks also include-whether a person had directly held a participation of more than 50% in the capital of an LLC that was struck off the CR without winding-up. Though these can be further strengthened, the aforementioned checks can act as a barrier to entry and limit the possible abuse of legal persons. Indeed, the CR did confirm that over the years there were a small number of applications for registrations that were turned down on this basis.

459. Checks with regards to sanctions are not carried out at this stage though authorities have advised the AT that there have been instances where these were then carried out by the Ministry for European and Foreign Affairs (MFEA). However, this does not appear to be done on a systematic basis.

460. Identity checks are carried out with regard to the founders when the LP is being established. Where the LP formation is carried out through a notary, the notary would be carrying out CDD on the founders whereas where the establishment of an LP takes place through SPOT, the founder needs to present an identification document and have the signature on the statutory documents presented with the application certified by a notary as well. Additionally, reliance is made also on the interconnection of the SBR with the Central Population Register (CPR) and the Tax Registry (TR) to ensure that details reported for involved parties are consistent, including for non-resident shareholders who are equally required to register with the tax authorities.

461. The SBR and CR thus provides users basic information and documents on the LP, including its statuary documents, its legal representatives and its members, though not on anyone acting as director or in a similar position who is not authorised to represent the legal person. The membership of joint stock companies (JSC) is represented in dematerialised form on the Central Securities Clearing Corporation (CSCC), the country's Centralised Securities Depository, rather than being reported on the SBR. Membership information must be updated within set time frames whenever there are changes thereto. However, following registrations there are close to no proactive checks made to ensure the detection of either late submission of updated information or the non-submission of information that is no longer relevant. When cases are detected by being brought to the attention of the authorities, action is then taken by the Ministry for the Economy and by the Market Inspectorate. However, the data provided on their activities did not concern supervisory and enforcement measures related to changes in basic information.

462. LPs also have to submit an annual report to AJPES, the timely submission of which is also monitored by AJPES. Authorities have confirmed that the submission of the annual report is often a triggering event for LPs to seek to update their basic information. Apart from updates carried out in this manner, reliance is otherwise put on the CDD measures carried out by OEs at on-boarding and on an on-going basis. This is especially the case with banks, as in excess of 95% LPs hold a local bank account. While this may provide some reassurances that changes to LPs are being monitored, it means that the SBR is dependent on the quality and timeliness of OEs' AML/CFT measures. This control is not particularly effective when it comes to foreign LPs present on the SBR as only roughly 60% of them retain a bank account in Slovenia.

463. Every LP established in Slovenia has to report information on its BOs to the RBO and keep it up-to-date. Information in this regard has to be communicated to the RBO within eight (8) days from registration and, once registered, within eight (8) days from when a change in BO information takes place. When the requirement of BO disclosure was introduced, authorities undertook a series of actions to ensure that the RBO would be fully and correctly populated, including training sessions for OEs by the OMLP and data analysis by FARS to identify possible defaulting LPs and informing them of the BO disclosure requirements. There were cases where authorities even undertook misdemeanour procedures against certain LPs that failed to comply with these requirements.

464. However, the RBO or AJPES have no powers to conduct checks to ensure that newly registered LPs are disclosing BO information to the RBO within the required timeframe, that they are making the right determination as to who is to be reported as BO, and that the latter's identification is correct. These checks are left to be carried out by the OMLP and FARS through their supervisory activities. Identification-related issues are also mitigated through the interconnection with the CPR and the TR, but this would not necessarily entail that a non-resident identified as a BO would be covered. Considerable reliance is also put on OEs who, as part of their CDD, have to ascertain that the LP has effectively disclosed its BOs to

the RBO, that it has done so correctly, and that it has kept the information up-to-date. The nature of the checks carried out do not fully ensure that BO disclosure obligations are effectively being adhered to.

465. OEs are to report identified discrepancies to the OMLP, and the latter, where it considers that it is justified, contacts the LP to remedy the reported discrepancies. While the OMLP has the powers to also carry out checks on the accuracy of the information disclosed to the RBO at its own initiative, such checks have been few and far in between due to the resource constraints the OMLP faces. Over the assessment period, overall the OMLP carried out 533 procedures to ascertain the accuracy of BO data reported to the RBO, and while the OMLP indicated that there were some carried out on its own initiative, the vast majority resulted from discrepancy reports submitted by OEs in the financial sector, primarily by banks.

466. The OMLP's activities in this area are supplemented by checks carried out by FARS in the context of tax inspections, and by other supervisory authorities. However, this still results in limited coverage and does not ensure a risk-based approach to a proper review of the disclosures to the RBO. FARS has undertaken a total of 533 checks on LPs, the BoS through its sampling has considered additional 342 LPs, while the OMLP through its various supervisory roles has covered a total of 2 459 LPs. These would represent 4% of the LPs included in the RBO.

467. Moreover, the number of LPs currently present on the RBO do not tally with the number of LPs within the SBR. This mismatch can be partly attributable to the following: while some LPs are not required to register in the RBO, there is still a number of LPs, including single member companies, that are yet to be included in the RBO due to technical issues; at the same time, the SBR also features some LPs that need to be struck off due to their inactivity. With regards to the single member companies missing from the RBO, the respective information on the BO would still be accessible through the SBR but this would not include information on anyone else exercising control over the LP.

468. In addition to tax-related checks carried out at the pre-registration stage as referred to above, the inspections carried out by FARS as part of its tax-related mandate are another measure that limits the abuse of LPs. FARS seeks to identify possible LPs that may be involved in tax evasion and/or tax fraud on the basis of a series of indicia and data sets. By way of example, it takes into account whether an LP registered for tax purposes is carrying out any actual economic activity; whether there are abrupt or unexplained changes in ownership, management, activity or transaction volumes that are inconsistent with its economic activity; use of foreign legal representatives or foreign BOs, combined with a structure that limits transparency and traceability; etc. Of the circa 5,800 inspections carried out, it confirmed irregularities in 4,838 cases where it cancelled the VAT registration of the LPs concerned. The results of the checks carried out are communicated to the Ministry for Economy for possible action from their side.

469. Given the reliance on the OEs and LPs for the accuracy of information in the RBO, through its outreach activities, the AJPES and the OMLP have made efforts to educate both OEs and LPs as to the BO disclosure obligations. Nevertheless, given the instances of unreported discrepancies by OEs (see under Section 5.3), further awareness raising, especially among the OEs, would be advisable.

470. Nominee shareholders and nominee directors are not concepts recognised under Slovenian law. At the same time, shareholders of a public limited company who are entitled to participate in the general meeting have the right to authorise as a proxy a natural or a legal person with the capacity to contract, to participate in the general meeting in their name and exercise their voting rights (CA paragraph 6 Article 308). A proxy with a written authorisation may vote on behalf of an LLC member (CA 2. Paragraph, article 506). Shareholders of a public limited company who are entitled to participate in the general meeting have the right to authorise as a proxy a natural or a legal person with the capacity to contract, to participate in the general meeting in their name and exercise their voting rights (CA paragraph 6 Article 308). A proxy

with a written authorisation may vote on behalf of an LLC member (CA 2. Paragraph, article 506). Allowance for nominee arrangements is made in the context of the CSCC where legal professionals are allowed to hold under escrow securities for a short period of time until they finalise particular transactions. However, the presence of strawmen was something that LEAs did comment about, and which is encountered in the course of their investigations. Thus, the provisions of law do not seem to be a sufficient deterrent to prevent such informal arrangements whereby one natural person formally acts as a director or shareholder on behalf of another person with no transparency as to who the shadow director or shareholder may be.

471. The SBR does allow for the detection of possible instances where several LPs share the same address or legal representatives. This notwithstanding, there have been very few sporadic instances where the analysis of the address and legal representatives data was undertaken to identify possible vulnerabilities and risks in the current system, or to inform the risk understanding of the authorities. The one exception is FARS which makes use of these checks as part of its mechanisms to identify possible cases of tax evasion as already referred to above.

5.3. Legal persons: Timely access to adequate, accurate and current basic and beneficial ownership information

472. Basic and BO information is available to all competent authorities in Slovenia through online access to the SBR and the RBO. Basic information on companies accessible through the SBR includes data and information allowing for the identification of the LP itself (e.g. name, registered office address, registration number), the individuals and entities that are its legal representatives and/or shareholders, as well as information on their basic powers. In the case of JSCs, information on membership is available through the CSCC.

473. The basic information should be kept current at all times but the absence of any timely and proactive oversight and the limited application of any sanctions for late or non-filing of updated information casts doubts about the accuracy of the information available through the SBR. For example, instances have been uncovered by FARS of 53 LPs allowed to remain active even though they do not have a legal representative. As regards the CSCC, in the case of nominee accounts held by legal professionals, much would depend on the CDD measures carried out by the legal professional concerned.

474. With respect to other LPs (i.e. associations, foundations, political parties, trade unions and religious organisations), the relevant laws do provide timeframes within which changes to their basic information is to be communicated to the respective register and, by implication, to the SBR. However, the absence of data on whether there were any late or non-submissions, and the corresponding actions taken, including the imposition of sanctions for any such failure, did not allow the AT to come to a conclusion about the effectiveness of the existing legal framework.

475. The information on BO available through the RBO is quite extensive, including information on the identity of the individual/s identified as BOs, information on the LPs involved, and information on how BO is being exercised. In addition, authorities can also access historical information on BO. All competent authorities have direct access to the RBO and its flexible search facilities allow them to search the RBO either by individual or by entity.

476. However, as acknowledged by LEAs, Prosecutors, and the private sector, the data obtained through the RBO is not considered fully reliable as there have been instances where the individuals identified as BOs did not coincide with those considered as such by the authorities or OEs. Concerning the accuracy and timeliness of information reflected in the RBO, the responsibility for providing and updating BO

information, as well as for verifying its accuracy, rests with the LP. The fact that the RBO and AJPES have no powers to carry out checks to ascertain that this is actually done by LPs is a significant shortcoming in this regard.

477. As a means to ensure that all LPs comply with their BO information disclosure obligations, Slovenia requires OEs not to engage in business relationships with, or carry out transactions for, customers that cannot prove they have submitted their BO information to the RBO. In addition, where BO information has been provided, OEs are also obliged to report any discrepancies they come across between the BO information reported in the RBO and their own determination and identification of BO. Any such discrepancy is to be reported and acted upon by the OMLP. Not all discrepancies are communicated to the OMLP, as it informed the AT that they have directed OEs not to disclose minor discrepancies (e.g. an outdated address or typographical errors) as long as the situation is not high risk or there is no suspicion of BO concealment.

478. However, meetings with the private sector informed that discrepancies are not always reported independently of their severity. While this may equally result in the updating of information in the RBO where the OE insists on it to service the LP, it does not necessarily mean that this will be always the case, nor that it will be done within an acceptable time-frame.

479. The absence of any similar obligation on competent authorities is a further limitation on the safeguards in place to ensure the quality of the information in the RBO. As already indicated, LEAs state that they are encountering situations where the actual BO is someone other than the individual(s) indicated in the RBO. Apart from discrepancies they come across through their own activities, authorities also have access to information obtained from foreign counterparts which may also be used to carry out cross-checks with RBO data and ensure the accuracy of the data reported in the RBO.

480. Another possible source of BO information is the Bank Account Register (BAR). Data on accountholders would, where applicable, also include information on the BO(s) thereof. The BAR is linked to the RBO, limiting the possibility of any BO(s) being entered unless they correspond to those identified as such in the RBO. In the event of any discrepancy between the two, it is left to the reporting institution to seek the resolution of the issue and possibly report the discrepancy to the OMLP.

481. Competent authorities also rely on other sources of information on basic and BO information of LPs. Where necessary, LEAs obtain basic and BO information directly from the LPs, although no information has been provided on how frequent this is the case. However, the absence of any coordinated and proactive supervision as to how LPs abide by their obligations, together with cases where incorrect information was reported by the LPs to the RBO puts into question how reliable the BO information may be.

482. OEs constitute another useful source of basic and BO information. Most OEs, especially those in the more material sectors like banks, showed a good understanding of BO-related obligations and how they determine who is the actual BO, including by basing their conclusions not only on customer declarations, legal documents and searches in the registers, but also employing third-party RegTech solutions and open data sources. Besides reports on identified discrepancies submitted to the OMLP, OEs provide information on LPs to the OMLP upon the latter's request. While the AT was not provided with any data as to how many requests for information it has submitted to OEs involving BO-related data during the period under review, the OMLP has confirmed that it has always received a reply to every request for information it has ever submitted to OEs. BO information is also provided by OEs when submitting STRs. LEAs can also obtain this information directly from OEs, but, similarly, there is no information on how often this information is sought from this source. Supervisors, when necessary, obtain BO and basic information on LPs from OEs as part of their supervisory activities.

5.4. Legal arrangements: Timely access to adequate, accurate and current basic and beneficial ownership information[22]

483. The ability of competent authorities to have timely access to basic and BO information of legal arrangements could not be assessed, as authorities do not consider legal arrangements as a phenomenon that is present in Slovenia with any regularity; the authorities very rarely encounter them in the carrying out of their functions. This was also corroborated through meetings with the private sector.

484. This notwithstanding, competent authorities would still be able to access BO information through the OEs as the latter have an obligation to obtain BO information when servicing trusts and similar legal arrangements, as do trustees (although their presence and that of TCSPs in general is not acknowledged by the authorities). Trustees have equal obligation to report BO data to the RBO. However, there are no such legal arrangements reported in the RBO.

5.5. Effectiveness, proportionality and dissuasiveness of sanctions

485. Authorities have a number of measures available to them to sanction breaches of basic and BO disclosure requirements. The main sanctioning tools consist in fines which can be imposed by (i) the Ministry for the Economy when it comes to failures related to the disclosure of basic information under the Companies Act; (ii) FARS and OMLP under the APMLTF-2 in relation to failures related to the disclosure of beneficial ownership information; and (iii) AJPES when it comes to the specific failures related to the filing of the annual report. These fines can be imposed through the misdemeanour procedure under the Minor Offences Act, which also makes allowance for the imposition of warnings or reprimands instead of fines. In addition to the above, companies that are considered as inactive can be struck off. In the light of the data provided by Slovenia on the application of these sanctioning tools , it cannot be considered as evidence of effective, proportionate and dissuasive sanctions as overall they have been limitedly applied.

486. As the main enforcement mechanism under the Companies Act (CA) to ensure adherence to basic information disclosure obligations, a company that fails to meet its reporting requirements may be subject to a misdemeanour procedure which may result in the imposition of a pecuniary penalty ranging from EUR 1 000 to EUR 45 000 (CA, Art. 685), depending on the particular classification of the company. Misdemeanour procedures in this case are administered by the Ministry for the Economy, which has had recourse to this procedure a number of times over the assessment period. However, the misdemeanour procedures undertaken did not relate to failures relating to the timely updating of basic information, including the 53 cases of LPs without a current legal representative referred to above, but mostly related to other requirements arising from the CA.

487. The above may be a consequence of there being no systematic mechanism to monitor adherence by companies with their information reporting requirements. By way of example, any public authority that comes across situations where official correspondence cannot be delivered to the company's registered address are to highlight these cases to the Ministry for Economy for it to take enforcement action. The options available to it is to order remediation and undertake a misdemeanour procedure or, in the case of a company, refer the matter to the CR for the company's eventual strike off. While the AT was informed that there were instances where misdemeanour procedures had been undertaken against LPs due to this particular issue, the only provided data related to two misdemeanour procedures undertaken following

22 See the Methodology for Recommendation 25 regarding beneficial ownership information for legal arrangements.

flagging by MIRS. No data on the total number or the actual value of pecuniary penalties and/or warnings that were imposed on the LPs concerned and their responsible persons was provided.

488. AJPES is also entrusted with administering misdemeanour procedures when it comes to LPs' failure to file their annual report. The pecuniary penalties that can be imposed in this regard are lower than those described above, ranging from EUR 500 to EUR 30,000 in the case of companies (CA, Art. 686). Data provided for 2024 shows that there were 1 241 cases in which a misdemeanour procedure was carried out with regards failures related to the annual report, resulting in 462 pecuniary penalties and 799 official warnings. However, the data provided does not allow for any analysis on whether the resulting penalty was proportionate to the seriousness of the case in question as neither is a reference made to the value of the pecuniary penalty nor to the time lapse until the annual report was filed by the LP in question.

489. As regards the striking-off of LPs, a total of 3,370 legal entities were struck off under the Financial Operations, Insolvency Proceedings and Compulsory Dissolution Act, out of which 3,194 were LLCs. The main reasons for the application of this procedure are related to the cessation of activities by the LP. While this can be an effective measure to keep the SBR (and consequently the RBO) as up-to-date as possible, the cessation of activities by LPs is not proactively monitored by authorities but depends on cases being brought to their attention. In addition, the data from any such striking off is only limitedly made use of through the checks carried out by the CR at the registration stage.

490. LPs that fail to meet their BO disclosure obligations are equally subject to pecuniary penalties which can be imposed by either the OMLP or FARS through the misdemeanour procedure, i.e. a procedure of a criminal nature undertaken in terms of the Minor Offences Act. Pecuniary penalties range from EUR to EUR 3, 000 to EUR 120, 000 for the LP and from EUR 400 to EUR 2,000 for the LP's responsible person.

491. The extent to which the two authorities have exercised this power varies, depending also on the extent of the supervisory activities undertaken. In the case of the OMLP, there were 7 cases over the review period where it considered that recourse had to be had to the misdemeanour procedures resulting in the imposition of 1 decision, 7 warnings and one pecuniary penalty. The one instance where a pecuniary penalty was imposed – EUR 3 000 on the LP and EUR 400 on its legal representative – related to a failure to provide BO information to the OMLP. FARS had recourse to the misdemeanour procedure in 15 cases resulting in the imposition of 4 official warnings and a total of EUR 29 000 in pecuniary penalties.

492. The authorities' exercise of their sanctioning power is therefore quite limited. While both the OMLP and FARS stated that there were other cases where BO discrepancies were detected, they also considered that the LP had remedied the discrepancy in the course of the supervisory process and therefore it was not considered that additional enforcement action was warranted. Authorities expressed a preference for remediation rather than sanctioning so as to ensure that the RBO would be properly populated. However, from the case-studies provided by FARS, it is clear that there were cases where serious BO discrepancies were identified, including cases where no BO or the wrong BO had been reported, but still no enforcement action was taken.

493. Even where the misdemeanour procedure was applied, the resulting pecuniary penalties imposed were not particularly high. Notwithstanding the absence of granular statistics on the matter, the deficiencies identified by FARS in 13 cases concern violations relative to the registering of the BO, updating the reported information, and filing incorrect information while the other two instances related to not responding to a request for information from competent authorities. However, the pecuniary penalty imposed for BO deficiencies would on average total EUR 1,934.

494. The authorities have signalled that they are now moving towards a more robust enforcement approach and in 2025 the OMLP imposed two pecuniary penalties for BO deficiencies, including a case

where a nominee was disclosed as the BO. This change in the approach is also reflected in the revised guidelines issued by FARS to its inspectors in August 2025. While inspectors for both the OMLP and FARS enjoy considerable discretion as to how to approach issues that may be detected in the course of their work, FARS' revised guidelines stress the importance of also making use of sanctioning measures rather than focusing mostly or only on the remediation of the issues identified. However, this change in approach is still in its early days, with the AT being unable to assess whether this will result in a better and more effective use of the enforcement powers available to the authorities.

495. The misdemeanour procedure under the Minor Offences Act may in itself prove to be an obstacle to proportionate, effective and dissuasive sanctioning as it entails that anyone who decides not to appeal the authority's decision and settles within eight days benefits from a 50% decrease and the possible implications of the four (4) year prescriptive period can result in cases involving serious breaches of one's obligations going unpunished. One feature that can have a positive impact is that the misdemeanour procedure requires a responsible individual be identified and sanctioned, in order for the LP to be subjected to some form of enforcement action. However, the compulsory nature of this requirement can also inhibit the authorities from making a more robust use of the misdemeanour procedure against LPs.

496. As regards OEs, misdemeanour penalties are also applicable when AML/CFT obligations with respect to BO are not fulfilled. Although there have been some instances in respect of which penalties have been imposed for failures related to BO obligations, the number of breaches related to BO obligations arising from supervisory examinations is minimal. Additionally, as remarked under IO.3 and IO.4, the sanctioning system was not considered as resulting in the imposition of proportionate, effective and dissuasive sanctions.

Chapter 6. Financial Intelligence

The relevant Immediate Outcomes considered and assessed in this chapter is IO.6. The Recommendations relevant for the assessment of effectiveness under this chapter are R.29-32 and elements of R.1, 2, 4, 8, 9, 15, 34, and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) The OMLP has access to a broad set of databases directly or indirectly upon request which enables it to perform its function. LEAs and prosecutors are generally able to gather necessary financial information and intelligence, even though recent legislative changes restricted their direct access to banking data of natural persons, requiring a higher evidentiary threshold for obtaining a requisite court order in this respect. The information contained in databases is relevant, accurate and up to date, although the RBO and SBR in some instances lack accuracy.

b) The OMLP has operational independence and autonomy to carry out its functions. In 2021-2022, the political context in the country had an impact on the operational autonomy of the OMLP, which allegedly affected the integrity of its analytical and dissemination processes. Subsequent measures implemented by the authorities, including internal reviews and changes in the management of the OMLP as well as investigations launched by LEAs, addressed these issues and led to effective reinstatement of the OMLP's operational autonomy.

c) STRs and CTRs are received electronically in the OMLP case management system. The Police submit initiatives which are also treated as STRs. However, in the absence of an automated mechanism, the incoming cases are assessed manually for prioritisation, which is not efficient. While the number of STRs/initiatives received by the OMLP have increased, the number of ML disseminations originating from STRs, other than those related to online fraud, have not risen in proportion thereto primarily due to resource constraints and shortcomings in its manual prioritisation mechanism, contributing to a backlog of cases. In the analytical phase, the case is enriched, and where appropriate the decision is taken to disseminate the case to the competent LEA. OMLP disseminations are used to some extent to support the operational needs of LEAs when pursuing ML or predicate offences and tracing assets.

d) The OMLP prioritises TF-related STRs, handles them with urgency and ensures timely dissemination to the police. There is a dedicated staff dealing with the TF related matters in the OMLP.

e) Strategic analysis is carried out to a limited extent. The absence of a dedicated fulltime strategic analyst, combined with the lack of STRs from DNFBPs and FIs besides banks as well as the lack of data mining and analytical tools, restricts the OMLP's capacity to systematically process large volumes of information, identify emerging trends, and detect evolving ML/TF typologies.

f) The OMLP closely and effectively cooperates with other competent authorities and exchanges information, including through cooperation with LEAs and prosecutors in the format of the special investigative teams. However, issues observed in relation to confidentiality and security of the process for dissemination of financial information and intelligence by the OMLP, which is done in hard copies, raise concerns, especially with respect to disseminations sent via the post to local police units.

Key Recommended Actions (KRA)

a) The OMLP should enhance its mechanism of prioritisation of STRs and other initiatives in line with identified risks in order to increase efficiency in operational analysis and ML dissemination originating from STRs. It should furthermore improve the existing methodology for conducting operational analysis to ensure the quality and consistency of the analyses produced.

b) The OMLP should expand its human resources capacity with requisite expertise as well as increase its technical capabilities for both operational and strategic analysis.

Other Recommended Actions

a) The OMLP should regularly conduct strategic analysis and make use of the information available in its databases in order to identify new typologies and evolving trends.

b) The OMLP, the Police and the prosecutorial authorities should ensure the confidentiality and timeliness of exchanges of financial intelligence including by implementing a dedicated, secure electronic channel to ensure the information is handled with strict observance of its classification level throughout the process by all authorities involved.

c) Slovenian competent authorities should have clear procedures and deadlines to provide feedback to OMLP on the quality and utility of intelligence disseminated by the OMLP in relation to ML/TF and predicate offences. The feedback should be timely and systematically provided to and analysed by the OMLP.

d) The OMLP should ensure that training and feedback is provided more regularly to all DNFBPs to further raise their awareness on AML/CFT in order to increase submission of STRs from the non-financial sectors.

Overall Conclusions on IO.6

The OMLP, being operationally independent and autonomous, has extensive and timely access to a broad range of databases enabling it to perform its functions. While LEAs have also direct and indirect access to various databases, recent legislative amendments limit their access to banking information and hinders their effective performance.

The OMLP produces and disseminates operational analysis which is used to support operational needs of other competent authorities to some extent. The insufficient resources and the shortcomings in its manual prioritisation mechanism for STRs limit the OMLP's ability to produce financial intelligence in a timely manner, particularly with respect to ML cases, which is a major deficiency. The OMLP effectively prioritises TF-related STRs and ensures timely dissemination to the police. While strategic analysis is produced to some extent, the absence of the relevant methodology and dedicated fulltime staff coupled with the gap in STRs from DNFBPs and FIs besides banks hinders the OMLP's ability to detect and follow evolving ML/TF trends and typologies.

The AT has placed importance on the OMLP's good and regular cooperation with other competent authorities, particularly with the Police, including through special investigative teams. Nevertheless, its results have not yielded the corresponding number of criminal investigations initiated for ML. Certain shortcomings are observed in relation to confidentiality and security of the process for dissemination of financial information and intelligence by the OMLP, especially with respect to disseminations sent via the post to local police units.

Slovenia is rated as having a moderate level of effectiveness for IO.6.

6.1. Timely access to relevant, accurate and up-to-date information

6.1.1 By the FIU

497. The OMLP is acting as the central authority for receiving STRs, CTRs, reports on wire transfers to higher-risk countries as well as on cross-border cash transport and BNIs. These reports are stored in OMLP's own databases (ISUPPD). The OMLP also has extensive and timely access to a broad range of databases directly or indirectly upon request.

498. The OMLP makes regular use of information contained in databases for its operational analysis. They have direct access to a wide range of databases: evidence of persons suspected to commit criminal acts, cadastral evidence of real estate register, eCRP (central register of population), register of issued tax number, eTAX register, evidence of real estate including claims, employee databases, central register of trade with securities, ePRS (Slovenian Business Register), eRTR (Bank Account Register), JOLP (Annual reports of companies), RBO. Besides these, they can have timely indirect access to central register of convicted persons, central register of loans, vessels register, aircraft register.

499. The challenges relating to accurate and up-to-date information (see IO.5) in the RBO and SBR are applicable here and can hinder the OMLP's ability to accurately identify the individuals who ultimately own or control legal entities. This, in turn, constrains its capacity to trace the flow of illicit funds, uncover links between seemingly unrelated entities, and detect complex criminal networks. Nevertheless, in specific cases where there are concerns on the reliability of BO information, the OMLP uses its powers conferred by the AML/CFT Law, seeking to address these challenges by requesting (via email) BO information from obliged entities, especially banks, to cross-check the data from the RBO and form a comprehensive understanding during its analysis. This happens on an ad-hoc basis and is not standard practice.

Types of reports received

500. The OMLP is the central authority for receiving and analysing STRs from OEs. Between 2020 to 2024, the OMLP received 4799 STRs. During the assessment period, most STRs were submitted by financial institutions, with roughly 82% of STRs originating from banks. Most of the STRs relate to ML (4659 STRs or ~ 97%), while a small percentage is related to TF (140 or ~3%), which adequately reflects the country's risk profile as set out in the NRAs (see table 6.1 below).

501. The number of ML-related STRs from OEs has increased significantly since 2023. No breakdown of full statistics for the past few years on predicate offences reported in STRs are available, as OEs are not required to identify the predicate offence when filing STRs. Moreover, the current STR template does not

include a dedicated field for this information that would allow for generating the full statistics on predicate offences reported in STRs. However, based on the STR analysis carried out by the OMLP resulting in disseminations and feedback received from LEAs on disseminated cases the OMLP estimates that in the last years, the most frequent predicate offences associated to ML STRs were fraud, tax evasion, abuse of position of trust in economic activity. This is largely consistent with the 2025 NRA, which identified economic crime (including abuse of position of trust and tax evasion) as the main ML threat while classic property crime (which includes online fraud and attack on an information system) is the third main threat of ML.

502. The number of TF-related STRs has fluctuated in the reviewed period. Most of the STRs related to TF were submitted by payment service providers and by banks. No TF-related STRs have been submitted by DNFBPs. The low volume of STRs related to TF is consistent with the country's low risk of TF and can be caused by the lower level of understanding of TF risks by some OEs (see IO.3 and IO.4).

Table 6.1: Breakdown of STRs received

	2020		2021		2022		2023		2024	
	ML	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	**TF**
Banks	737	5	732	6	776	4	762	2	901	11
Savings institutions	87	1	57				102	1	143	2
Post Office	17		4		1		1			
Brokerage companies and management companies of investment funds	4		3		1					
Leasing	1		1		3		1		4	
Auditors and accountants			1				3			
Casinos	1						1		4	
Other organisers of games of chance	1				3		6			
Dealers with precious stones			1		4		2		2	
Real estate agencies					1					
Insurance companies	1								2	
Virtual currencies			6						8	
Payment service providers	38	45	23	13	32	30	32	16	25	4
Other obliged entities/EMIs	4		29		17		32		35	
Notaries	1		1		1		2			
Covered lawyers	1		2		1					
STRs (total)	**893**	**51**	**860**	**19**	**840**	**34**	**944**	**19**	**1122**	**17**

503. Banks consistently submit the highest number of reports annually and the quality of their reports is assessed as high by the OMLP. In the absence of the dedicated field in the form, FIs usually describe the underlying crime in the narrative part of their STR and in the process of the analysis the OMLP checks if the categorisation is correct. When STRs lack sufficient information, the OMLP requests additional information from OEs via email and FIs usually reply within two days (i.e. well within the prescribed maximum time-limit of five days under APMLTF-2). Nevertheless, STRs submitted by banks rarely need additional information or clarification, in contrast with the ones received from other FIs and DNFBPs. Generally, the OMLP has the good practice of providing feedback to OEs: a) immediately after an STR is received to indicate possible deficiencies or missing information; b) when it concludes a case to inform the OE about the findings of its analysis; and c) once a year, as part of feedback to banks and savings banks.

504. DNFBPs, despite being exposed to ML/TF risks, report very few suspicious transactions, which seems to be linked to their insufficient understanding of ML/TF risks (see IO.4). The low number of STRs

submitted by DNFBPs reduces the diversity of intelligence available to the OMLP and narrows its capacity to identify potential ML/TF cases, since their reports are essential for uncovering complex financial schemes that may not be visible through the banking system alone. Although between 2020 and 2024, the OMLP has delivered trainings to DNFBPs, including tax advisors and accountants, traders in gold and precious metals, real estate agencies, notaries and covered lawyers to raise their ML/FT awareness, these initiatives have not yet been reflected in increased STR reporting across DNFBP sectors.

505. The OMLP also receives information ("initiatives") from state authorities that include the Police, the FARS, the Prosecutor's Office, the Courts, and the SOVA. These are treated as STRs by the OMLP, although they can be rejected if they are not sufficiently substantiated or do not contain elements of ML or TF. Most initiatives come from the police and have been increasing because of growing number of online fraud cases detected by the police. In these instances, the police refer cases to the OMLP due to its powers to temporarily suspend transactions for 72 hours and its efficient access to banking and transaction data. The OMLP explained that while it was able to stop some fraudulent transactions because of police initiatives, the large volume of received online fraud-related initiatives is burdening the OMLP's already limited resources and ability to review STRs in a timely manner. Some of the fraud initiatives are submitted with a delay to the OMLP, reducing the chances to stop transactions in time. Also, a significant proportion of them involve transactions of low value, that do not always justify the allocation of OMLP resources.

506. In attempt to reduce the number of online fraud initiatives referred to them which stretch their already limited resources, in the guidelines adopted in September 2025, the OMLP introduced certain criteria for rejecting initiatives. The criteria include a combination of the value of a suspicious transaction, the time lapse since the transaction and whether or not funds have been transferred abroad. As an example, initiatives related to transactions abroad that are below EUR 1,000 submitted three days after the transaction would be rejected. As a consequence, in 2025, out of 900 initiatives received, the OMLP rejected 130. Also, it should be noted that some of the online fraud-related initiatives are duplicated by STRs, since a victim first approaches the bank (which then submits the STR) and subsequently the Police (which then submits the initiative). While the OMLP and the police have made some co-ordinated efforts to avoid duplication, this still cannot be fully avoided.

Table 6.2: Breakdown of cases initiated by OMLP based on received initiatives, foreign requests, etc.

	2020		2021		2022		2023		2024	
	ML	**TF**	**ML**	**TF**	**ML**	**TF**	**ML**	TF	**ML**	**TF**
Initiatives from state authorities (total)	**115**	**1**	**128**	**5**	**167**	**1**	**318**	4	**538**	
Ministry of the Interior, Criminal Police Directorate	70		99	3	142		289	2	509	
State Prosecutor's Office	17		9		6		6		6	
FARS			4							
Courts	3		4		2		11		14	
Commission for the Prevention of Corruption	1		1		1		2			
Slovenian Intelligence and Security Agency	24	1	11	2	16	1	10	2	8	
Office of the Republic of									1	

Slovenia for Budget Supervision										
Reports from supervisory authorities	**16**		**14**		**17**		**10**		**7**	
Securities Market Agency	1									
FARS	1									
Market Inspectorate			1							
Bank of Slovenia	13		13		17		10		7	
Insurance Supervision Agency	1									
Cases initiated by OMLP on its own initiative or by other means	**2**	**1**	**18**		**25**					
5. Foreign FIUs	**58**		**55**	**4**	**74**	**3**	**44**	**1**	**42**	**2**

507. The OMLP can request data from OEs and other state bodies when needed for the detection of ML/TF and predicate offences, which must be provided within 5 working days (by OEs) or 15 days (by other state authorities), unless indicated otherwise in OMLP's request.

508. The OMLP also receives the following reports: on average 45,000 CTRs/year for cash transactions exceeding the threshold of EUR 15,000; 22,000 reports/year on transactions exceeding EUR 15,000 related to high-risk countries; 69 reports/year on cross-border transportation of cash exceeding EUR 10,000 from customs authorities (FARS) – in accordance with EU Regulation 2018/1672 on controls of cash entering or leaving the EU. This data is stored in the OMLP's database (ISUPPD) and is used to support the analysis of STRs. Only in the first 3 years of the assessed period the OMLP opened 6 cases *ex officio* based on the data derived from CTRs, which is a modest number, given that Slovenia has a cash-intensive economy with a medium-high threat of ML derived from cash (the 2025 NRA). While the number of CTRs submitted by casinos may not seem fully in line with the medium-low risk level assigned to this sector under the 2025 NRA, as explained by the OMLP and the FARS, CTRs in question include all transactions during a single visit when the threshold of EUR 15,000 was exceeded either through a single or multiple transactions (cash ins and cash outs); in case of the latter, all transactions are reported. The AT considers that data from CTRs are not explored more in depth by the OMLP for both operational and strategic analysis.

Table 6.3. CTRs received by the OMLP during 2021-2024

Obliged entity	2021	2022	2023	2024
	Number	Number	Number	Number
Banks	35,358	43,451	39,998	37,963
Savings institutions	4,195	4,169	4,122	4,524
Casinos	3,410	3,875	3,856	2,308
Other	17	72	77	0
Total CTRs received	42,980	51,570	48,053	44,795
Total amount (EUR)	1,536,055,994	1,918,830,127	1,744,560,420	1,642,262,398

Source: OMLP's Annual reports

Table 6.4. Reported transactions over 15,000 EUR related to high-risk jurisdictions

	2020	2021	**2022**	**2023**	2024
Total no. of transactions reported	5,847	3,875	9,299*	35,548**	56,567**
Total amount (EUR)	676,304,817	635,412,734	832,217,361	3,861,955,811	7,600,350,811

509. FARS submits cross-border declaration reports as well as information on undeclared and falsely declared cash and BNI. However, it is not known to what extent they have been used by the OMLP in their analysis or if they have ever been used to open ML/TF cases (see also IO.8).

6.1.2. By other competent authorities

510. LEAs, prosecution, and judicial authorities also have access to a significant number of databases, either directly or upon request. Their access is timely, and the data is generally adequate. However, since the amendment of the Criminal Procedure Act (CPA) in August 2024, LEAs and prosecutors' access to the Bank Account Register for natural persons has been restricted, granting of which now requires a court order. The latter is contingent on demonstrating a higher evidentiary threshold – the existence of reasonable grounds for suspicion that a criminal offence has been committed. While in cases involving potential ML/TF, LEAs and prosecutors can acquire banking information of natural persons via the OMLP, the changes in the CPA significantly limit the ability of LEAs to obtain intelligence at the pre-investigation stage of predicate offences (see IO.7).

511. The police have direct access to their own databases (information on previous cases, population register), SBR and RBO, databases of employment and health insurance services, criminal records, dangerous substances and non-scheduled transports, vehicles data in European registers. In addition, they have indirect access upon request to several other database, including those relating to vessels, ownership of aircrafts, tax data, and real estate.

6.2. Production and dissemination of financial intelligence

6.2.1. Production of financial intelligence

512. The OMLP has operational independence and autonomy to carry out its functions.

513. The OMLP plays a key role in producing operational analyses, which it disseminates proactively or upon request to the competent national authorities and foreign FIUs. There are 28 staff members within the OMLP, 10 of which are employed in the Suspicious Transactions Sector ((STS), 9 analysts and the head of the Sector). Three analysts are specialised: one for international incoming requests, one for restrictive measures, and one for TF. The number of analysts, in the light of the number of STRs, is not sufficient, and the authorities are considering a new prioritisation mechanism under a revised methodology and a new STR template with more pre-defined fields allowing for increased automatisation of data analysis, which would enable them to handle the increasing caseload more efficiently. The OMLP advised the AT that they have requested two additional staff members to be hired in the STS, of which one is to be dedicated full-time to strategic analysis. However, the requested hirings are not yet confirmed, nor have they an impact on the effectiveness of the assessed period.

514. All STRs are electronically received by OMLP directly in its case management system (ISUPPD), which has been in place since 2017. Through a manual prioritisation process, the Head of the STS does an initial check of all received STRs, reading them one by one, which is not efficient. In practice, the Head of STS prioritises STRs if they require urgent action (e.g., in fraud cases where the proceeds could be recovered), are related to TF, if adverse media exists regarding the issue involved, are related to earlier

received STRs (seen as indicative of increased probability of criminality) or if the amount involved exceeds EUR 200,000. Prioritised STRs are assigned to an analyst, while the STRs assessed with a low level of priority become dormant until they are subject to brief checks by analysts and concluded.

515. The aforementioned methodology, while used in practice throughout the period under review, has been formalised only in September 2025 through the adoption of the respective guidelines for the STS. The AT deems the prioritisation methodology not entirely effective, as it adopts a binary approach, with STRs or initiatives being treated either as urgent or low priority, without giving consideration to cases of normal priority. Moreover, the AT concludes that the manual prioritisation of STRs consumes already insufficient human resources and heavily relies on individual judgement and expertise, increasing the risk of delays, human error, biased case selection, or missed opportunities.

516. The average time to analyse an STR depends on the type of offence suspected, the urgency and the complexity of the case. The OMLP advised that urgent cases (e.g. related to TF or fraud) are analysed within 2 days and referred to competent authorities if sings of potential criminality are detected (See Case Box 9.1). Complex ML STRs are analysed within 1-2 months. During 2020-2024, the average lifecycle of an STR (from receipt to dissemination) was 6 months. As the authorities advised the AT, this partly resulted from the long duration of processing STRs under the previous management (in 2021-2022) and party from a longer duration of the average time needed to conclude low priority STRs. However, the average lifecycle has shortened since 2022 (overall average of about 3 months), with an average processing time of ML STRs disseminated to LEAs being 2.2 months.

517. At the time of the on-site visit, the OMLP indicated that the STS is facing a backlog of 850 STRs from 2024 and 2025, primarily as a result of insufficient resources. They advised that the backlog largely comprised of cases that had been deemed as low priority by the STS at the time of initial prioritisation done by the Head of STS as described above. Replicating the approach taken for processing the backlog from earlier years, the OMLP plans to allocate these cases to analysts to perform basic checks and conclude them as *ad acta* or notify the LEAs, as appropriate. The AT is of the view that OMLP lacks sufficient resources to simultaneously process both the backlog and increasing number of incoming reports, which limits their ability to produce high-quality and actionable financial intelligence in a timely manner.

518. Although case examples reflect that the OMLP has the ability to prioritise certain cases, the AT considers that the absence of an automated prioritisation mechanism with multiple priority levels – particularly as the number of STRs continues to increase each year – may heighten the risk of human error and delay the identification of high-priority cases. Moreover, the OMLP did not have a formalised analytical methodology to guide its operational analysis until September 2025. In the absence of such formalised framework, analytical outputs were largely driven by the individual knowledge, experience, and professional judgment of analysts.

519. In practice, as OMLP explained, when conducting operational analysis, every subject from an STR is checked through its database and all other databases to which it has access. If the case under analysis involves a transnational element such as foreign individuals, companies or accounts, OMLP proactively liaises with foreign FIUs to collect data needed for its operational analysis. During January 2020 - June 2025, OMLP sent approximately 2235 ML requests for information to foreign FIUs, and 19 requests related to TF (See IO.2). The number of requests has significantly risen since 2023, demonstrating that the OMLP increasingly and regularly sought international assistance from foreign FIUs to enrich its operational analysis or to identify fraudulent funds abroad.

520. When the analysis of an STR is concluded, the analyst proposes to the head of STS that the case be disseminated to the competent authorities or be concluded *ad acta*. If the head of STS is satisfied with the

quality of the analysis, she approves the dissemination and passes on the case to the Director of the OMLP for the final approval. In case the analysis needs further information to substantiate the proposed conclusions, the case is given back to the analyst in charge to gather additional information and to enrich the analysis.

Case box 6.1: The OMLP's operational independence and autonomy

There was a period during 2021 to 2022 when political developments temporarily affected the OMLP's ability to function autonomously. The newly elected Government at the time appointed a new Director of the OMLP, which resulted in replacement of several key staff within the OMLP and alleged arbitrary collection (including from foreign FIUs) of information and intelligence against natural and legal persons for political ends. This allegedly affected the integrity of analytical and dissemination processes within the OMLP during his tenure. Following the election of new Government in 2022, the Director was dismissed and the new head of the OMLP was appointed through a transparent selection process for a standard five-year term.

Steps were taken to address previous issues: an internal review was conducted and findings regarding detected irregularities shared with the NBI, which resulted in opening a criminal investigation against the former Director; disciplinary proceedings were brought against staff involved in the alleged misconduct; cases concluded in 2021 were reassessed and the annual report for 2021 was revised with corrected data; earlier practices of closing cases without prior analysis were discontinued; guidelines were developed for the OMLP's analysts; and foreign counterparts were informed of any affected notifications.

Discussions during the on-site visit confirmed to the AT that the OMLP presently functions with full operational independence and is not subject to undue influence. The AT concluded that this situation reflected an abuse of power rather than a systemic issue in the appointment of the head of the OMLP.

6.2.2. Dissemination of financial intelligence

521. The OMLP disseminates information to LEAs spontaneously or upon request. Based on the offences identified during its operational analysis, the OMLP can disseminate information to the following competent authorities: (i) Criminal Police Directorate (Economic Crime Unit), the Prosecutor's Office and other NCAs –ML suspicions; (ii) the Criminal Police Directorate – for TF suspicions; (iii) other competent authorities (Criminal Police Directorate, FARS, etc.) – for suspicions on other criminal offences.

Table 6.5. Cases opened and concluded by OMLP between 2020-2024[23]

Year	Total no. of opened cases	No. of **ML/TF** disseminated cases to the Police and Prosecutor's Office	No. of disseminated cases related to **other offences**	No. of closed cases
2020	1 137	450	486	298
2021	1 103	493	872	516
2022	1 161	314	418	339
2023	1 340	599	258	303
2024	1 728	920	242	278
Total	6 469	2 776	2 276	1 734

522. The number of ML disseminations made by OMLP to LEAs has varied over the reviewed period, with a decrease in 2022 and a significant increase in 2024. This decrease in 2022 can be attributed to the changes in the management of the OMLP and related challenges as explained above (Box 6.1). Conversely, the OMLP explained that the increase in disseminations in 2024 is due to the considerable increase in ML cases related to less complex online frauds (stemming from both STRs and police initiatives), which were prioritised by the OMLP and disseminated in a swift manner.

523. Disseminations to LEAs thus predominately relate to online fraud. The OMLP's 2023 annual report states that it identified fraud as the most prevalent predicate offence in 66% of notifications, while in the 2024 annual report this figure rose to 88%. Tax evasion accounted as predicate offence in 3% of the ML disseminations from 2023, but less than 2% in 2024. In 2024, the attack of an information system and the abuse of trust in economic power represented the predicate offences in 3.50% of ML notifications. This landscape suggests disseminations are supply-driven, frequently reactive to STR flows and fraud initiatives received from the Police rather than risk-based or strategically targeted. The AT believes that the lack of a strategic approach led to the small share of ML disseminations related to tax evasion and abuse of trust in economic power as predicate offences, which is not fully aligned with the country's ML risk profile.

524. The AT observed issues in relation to confidentiality and security of the process for dissemination, which is done via the post. This is further described below.

Strategic analysis

525. The OMLP carries out strategic analysis to a limited extent. During the period under review, the following strategic analyses have been produced: (i) the use of debit and credit cards to withdraw cash at Slovenian ATMs during 2023–2024, highlighting evolving new methods in the laundering of illicit funds through cash-out operations; (ii) cash usage in Slovenia. The OMLP also advised that once a year, the analysis of CTRs, transactions related to high risk-countries, cash transfers across EU borders, and ML/TF concluded cases is also carried out for the purpose of the OMLP's annual report. There are no established methods how to choose topics for and conduct strategic analysis. The lack of STRs from DNFBPs and FIs besides banks limits the diversity of strategic analysis and detection of ML/TF typologies.

526. Currently, the OMLP does not have a fully dedicated analyst responsible for strategic analysis; the only analyst performing this function on the part-time basis also serves as an advisor to the OMLP's management. This combined with the lack of data mining and analytical tools, restricts the OMLP's

23 The table contains data per indicated year on the overall number of opened cases and those concluded by disseminations related to ML/TF, disseminations related to other offences, and cases closed without dissemination (*ad acta*). With respect to some years, the number of cases disseminated and closed is higher than the number of opened cases, which, as explained by the OMLP, is attributable to the following factors: in a given year, cases originating from earlier periods were also processed, including the disposal of the backlog; a single STR, depending on its content and elements of possible criminality indicated therein, may result in multiple disseminations.

capacity to systematically process large volumes of information, detect suspicious networks or patterns, identify emerging trends, and detect evolving ML/TF typologies.

527. The ISUPPD platform used by the OMLP enables the extraction of some Business Intelligence (BI) reports (such as: "the frequency of STR submissions by each bank", "no. of cases concluded by each analyst", "concluded cases segregated by type"), enhancing visualisation and supporting more effective management of existing workflows. The OMLP noted that 15 additional BI reports are currently under development, which have the potential to provide a broader overview of its activities. While their concrete contribution to strategic analysis cannot be evaluated, these reports represent a promising step toward enhancing the OMLP's analytical capabilities.

6.2.3. FIU financial intelligence supporting needs of competent authorities

528. Financial intelligence produced by the OMLP supports the needs of competent authorities (police and prosecutors) to some extent, despite the fact that both authorities consider OMPL disseminations to be of good quality. The statistics provided in the table below indicate that most ML pre-investigations are initiated by the police based on their own investigative work. In contrast, the number of pre-investigations triggered by OMPL disseminations remains considerably lower.

529. Prosecutors receive OMLP's reports only when they initiate a case, usually when they lead special investigative teams or when the OMLP has information that pre-trial proceedings are directed by prosecutors. In the latter case, the prosecutors may request necessary information from the OMLP directly.

530. The number of resulting ML investigations, prosecutions, and convictions is not proportionate to the number of ML disseminations made by the OMLP. The LEAs stated that this is largely because initiating stand-alone ML investigations requires demonstrating a link to a predicate criminal offence (see IO.7).

531. Annually, the OMLP receives data on how their financial intelligence has been used from the Prosecutor's Office, Police, and FARS. Feedback received by the OMLP on its disseminations is provided to analysts – either in Excel format or through the case management system – and serves as a reference database for monitoring the status of proceedings and for improving future analysis.

Table 6.6. Number of ML pre-investigations triggered by different sources of information

Source of pre-investigation	2020	2021	2022	2023	2024
triggered without prior complaint	50	42	65	111	250
triggered by complained, including OMLP disseminations	19	18	28	53	60

532. The OMLP's products are also used to support ongoing investigations whether domestic or cross-border. The authorities presented a particular case where the SPO and NPU used intelligence from the OMLP to enrich their cross-border ML investigation (See Case Box 7.2.). The Police use financial intelligence in various stages of ML/TF investigations, from initial case analysis to ongoing intelligence gathering. Authorities stated that cases disseminated by the OMLP have helped the police to identify connections between the suspicious transactions and known criminal activity, individuals, or criminal organisations. The OMLP's intelligence has also been instrumental to investigate the ownership and control of assets, leading to freezing and seizing of criminal property.

533. TF-related disseminations are also sent to the Criminal Police Directorate, which examines and forwards them to the NBI. Based on OMLP's findings, the police start pre-investigation and conduct further analysis, if needed (see IO.9). In some instances, the police have sent initiatives to the OMLP to initiate the collection of financial data and submit back enriched analysis.

534. The OMLP supports the operational needs of FARS by spontaneously disseminating reports on tax offences. A central unit within FARS receives OMLP's reports and evaluates them, after which the reports are prioritised and audits are triggered. Most of OMLP's reports relate to tax fraud and undeclared work. CTRs and transactions related to high-risk countries are also submitted by the OMLP to FARS on a monthly basis, according to an agreement concluded between them. These reports are used by FARS to perform risk analysis, financial investigations, supervision of taxpayers, supervision of cash declaration at border, supervision of compliance with the ban on cash payments exceeding EUR 5 000. The data is automatically inputted by FARS into a specially developed database (QlikView) to be analysed and used within tax risk mitigation strategies related to (i) transactions with offshore jurisdictions and (ii) high-net-worth individuals (HNWIs).

535. FARS also has the good practice of systematically reporting on the use of information received from the OMLP (see Table 6.7).

Table 6.7. Use of OMLP reports received by FARS

Year	2022	2023	2024
Total notifications received from OMLP	293	165	179
Audits triggered by OMLP notifications	201	127	101
Misdemeanour proceedings initiated against tax payers	206	126	112
Amount of fines imposed	EUR 549 300	EUR 276 450	EUR 324 323
Criminal charges against taxpayers as a result of OMLP notifications	14	11	5

6.2.4. Other competent authorities producing financial intelligence (where relevant)

536. 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 special investigative techniques. The NBI possesses its own intelligence-gathering capabilities to effectively support operational and investigative work. Moreover, it receives support from special units established within the Criminal Police Directorate: a special analytical unit working to collect data and develop intelligence and the ICT – a unit that is dealing with crypto assets analysis. ICT also serves as the national coordinator for crypto assets, providing expertise to local police units.

6.3. Cooperation and exchange of information/financial intelligence

6.3.1 Co-operation and exchange

537. The OMLP cooperates and exchanges information with the police, prosecutors, FARS and other competent authorities. The exchange of information is usually conducted through initiatives and requests from NCAs as well as disseminations from OMLP, which are sent by courier or post (see below). The OMLP is also part of special investigative teams created by prosecutors for the detection and investigation of ML, associated predicate offences, and TF. This enables real-time exchange of information and intelligence and enhances cooperation. During 2020-2024, the OMLP participated in more than 20 special

investigative teams for conducting ML investigations and 14 special investigative teams for conducting financial investigations for asset recovery purposes. In some cases, as authorities advised, weekly meetings were held to agree upon the manner of conducting financial analysis and investigations, which proved to be a useful way of cooperation.

538. The OMLP exchanges information with the BoS mostly through initiatives submitted by BoS. The number of initiatives submitted by ISA and SMA to the OMLP throughout the period under evaluation is modest. The OMLP also provides supervisory bodies with the data needed for licensing and with opinions related to the applicants, and also data in relation to supervised entities such as the response time of an obliged entity to an OMLP request, timeliness and quality of reporting, which are subsequently used in supervisory activities.

539. The cooperation between the OMLP and the FARS primarily consists of disseminations from the OMLP relating to tax offences and abuse of economic power, while the number of requests for information or initiatives from the FARS remains limited.

Case Box 6.2 Cooperation between the OMLP and the police

In 2018, the Police initiated an investigation into a case involving a fraud scheme. Fraudsters initially contacted a branch office of a company pretending to be the director of the headquarters and instructed an employee to transfer money to a designated account, which were subsequently transferred abroad. The Police closely cooperated with the OMLP, which was involved throughout the pre-investigation and prepared over 60 financial intelligence reports for the Police, providing valuable insight and assistance to develop evidence. The analysis of the transactions involved in the case allowed the Police to identify several money mules in Slovenia. The evidence collected was sufficient to secure a conviction and impose a sanction of three years' imprisonment.

Source: Police

6.3.2 Security and confidentiality

540. The OMLP has measures in place to ensure confidentiality and secure storage of information kept in their premises. Employees handling confidential information have to undergo security checks at the time of employment, which are conducted periodically. Access to the premises and system is restricted and protocols are in place, governing the use of databases.

541. All information exchanged between the OMLP, LEAs, Prosecutors, and supervisory bodies is subject to classification under the Classified Information Act, at one of the following levels: Restricted, Confidential, Secret, or Top Secret. The OMLP uses the "Restricted" level of classification when disseminating information.

542. There are, however, some concerns regarding confidentiality of the information during the dissemination process. The OMLP sends financial intelligence and information to the Police in hard copies, either through authorised couriers or the Slovenian Post – in cases of disseminations addressed to local police units located outside Ljubljana. Although the OMLP advised that the Slovenian Post has authorisations to handle information classified as "Restricted", the AT is not convinced that the information is protected accordingly to its classification level. Moreover, the OMLP could not assure the AT that such information is received exclusively by an authorised person/officer within these units, which raises concerns about the confidentiality and protection of data. Considering that ML/TF cases are generally time-sensitive and that physical dissemination process requires longer delivery time compared to electronic

means, such delays may reduce the immediate operational value of the intelligence disseminated.

543. The Police stated they may send initiatives to the OMLP via electronic means, but classified and sensitive information is sent in hard copies by couriers. The AT concludes that the lack of an electronic secure channel affects the timeliness and poses risks in terms of confidentiality of data exchange.

544. By contrast, when exchanging information with foreign FIUs and Europol, the OMLP uses electronic secure channels, namely Egmont Secure Web and FIU.net.

6.4. Using information/financial intelligence

6.4.1 Using information / financial intelligence for investigations and developing evidence

545. The Police use financial intelligence to conduct their pre-investigations or to develop evidence, identify assets and trace criminal proceeds related to ML, predicate offences, and TF.

546. The OMLP's products are used to some extent to initiate criminal investigations. However, the majority of ML investigations are still triggered by the outcomes of the investigations of predicate offending due to the high evidentiary threshold (see IO.7).

547. In instances when the police have already opened preliminary investigations, the OMLP's disseminations serve as valuable supplements, as the information therein can provide new leads, be used for cross-checking or to develop new evidence. The OMLP's reports are used for critical insights into suspicious financial flows and help identify links between criminal organisations and illicit financial activities. The Police use data from the OMLP that originates from foreign FIUs to build and develop targeted requests for mutual legal assistance in order to obtain evidence needed for the criminal investigations.

548. In cases where the dissemination does not lead to a ML investigation, the data contained in the report functions as an analytical resource. It is utilised by the police to track potential financial crime trends, identify potential criminal networks, or monitor suspicious activities, even if it does not directly result in a formal criminal case.

549. Intelligence from the OMLP can be used to identify or support investigations into predicate offences. Nevertheless, the extent to which this has been used is unclear because the authorities were not able to provide information to substantiate a different conclusion.

550. Competent authorities can also make requests to the OMLP to determine whether a person is "known" to the OMLP, response to which entails a yes/no answer from the OMLP upon a simple search whether the person of interest to the authorities is traceable in the OMLP database. During 2020-2024, the OMLP received 42 such requests, majority of which came from the police (26 requests), whereas the rest – from prosecutors (12 requests) and courts (4 requests).

551. At the investigation stage of criminal proceedings involving ML/TF, prosecutors and courts can request the OMLP to supplement the ongoing investigation with additional data and information as needed.

6.4.2 Using information / financial intelligence to assist in identifying and tracing criminal proceeds or instrumentalities

552. The OMLP plays an important role in the identification and tracing of criminal proceeds, particularly due to its unrestricted access to information on bank accounts and transactions. The OMLP also has the power to suspend transactions for up to three working days when there is a ML/TF suspicion. Over the

past three years, the OMLP has exercised these powers in 104 cases. In most of the cases where suspicious transactions were withheld for 72 hours, the prosecutors were able to obtain temporary freezing orders from courts, managing to secure assets pending confiscation (see also IO.8). In some of the fraud-related cases referred by the Police, the OMLP successfully coordinated with foreign authorities to freeze accounts or suspend transactions.

Table 6.8. Transactions suspended by the OMLP

Year	Cases	Total value (EUR)
2020	10	817 371
2021	5	603 897
2022	19	1 147 562
2023	37	1 763 798
2024	48	1 467 339

Source: OMLP Annual report

Chapter 7. Money Laundering Investigations and Prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.7. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 3, 30, 31 and elements of R.1, 2, 15, 32, 37, 39 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Slovenia has legal and institutional frameworks to identify and investigate ML offences. Specialist teams and capabilities have been developed within the police and SPO with responsibility for complex ML cases. ML investigations are triggered by various sources including parallel financial investigations. However, recent CPA amendments have raised the evidential threshold required to obtain banking information and order special investigative measures, which has an impact on the identification and investigation of ML offences.

b) Prosecutors mostly pursue self-laundering and third-party ML directly linked to predicate offences, reflecting prevailing judicial interpretations that require a predicate offence to be established before ML can be investigated and further prosecuted. Interpretation stated in the case law is a dissuasive factor in the investigation and prosecution of autonomous ML. However, the authorities recognise this issue and are taking some measures to remedy this deficiency though effective results have yet to be fully materialised.

c) Majority of ML cases are derived from fraud with some instances where ML involved property obtained through drug trafficking. Legal persons feature in ML cases, nevertheless, they are not regularly investigated and prosecuted. These results are to some extent in line with the country's risk profile. However, a disproportion exists between the number of predicate offences and the resulting ML investigations.

d) The sanctions imposed are not effective, proportionate and dissuasive. Undue delays in criminal proceedings further weaken the impact of sanctions, as they often lead to reduced penalties and contribute to a perception that sanctions are not proportionate, dissuasive and effective.

e) When ML convictions are not feasible for justifiable reasons, the authorities pursue predicate offence and apply non-conviction based confiscation.

Key Recommended Actions (KRA)

a) Slovenia should take steps to ensure that the standard of proof set by the existing and settled jurisprudence does not present an impediment in pursuing autonomous ML cases, and demonstrate effective identification, investigation and prosecution of such cases.

b) Authorities should undertake review of ML sanctions, its effectiveness and dissuasiveness, with particular focus on how delays in criminal proceedings result in lenient sanctions. Based on the findings, specific policy should be developed, with the objectives to reduce delays and ensure sanctions serve as an effective deterrent to ML activity.

c) Authorities should conduct a review across all competent authorities of the impact of the limitations on investigative powers during the pre-investigation stage of ML and associated predicate offences and address any identified deficiencies to facilitate the effective identification and development of ML cases.

Other Recommended Actions

a) Slovenia should ensure that sufficient resources are allocated to LEA and prosecutors to pursue more complex ML cases.

b) Authorities should develop a better understanding of the liability of legal persons for ML offence in order to proactively and properly investigate and prosecute them.

c) Authorities should continue undertaking steps to overcome procedural reasons for delays in investigations and prosecutions and improve the timeliness of case before the court.

Overall Conclusions on IO.7

Slovenia does identify, investigate and prosecute ML where predicate offending can be established to some extent in line with its risk profile. In all instances of acquisitive crime, the competent authorities carry out parallel financial investigations. Police receive mandatory training and regular upskilling in relation to financial investigations, with further capacity building provided to Prosecutors, the OMLP and Judiciary. The authorities have demonstrated a capacity for undertaking cross-border and complex investigations, particularly with regional partners, which have led to some significant outcomes.

However, there are certain challenges which affect overall effectiveness and call for major improvements in this area. The absence of autonomous ML attributed to the high evidentiary threshold set by jurisprudence, remains a key issue. Despite the fact that in spare instances this jurisprudence is challenged, particular weight to this issue is given due to its impact on the effectiveness and timeliness of pursuing this type of ML. Sanctions for ML remain insufficiently dissuasive and effective. The persistence of this issue throughout the assessment period with little if any attempt to rectify them, suggest a lack of prioritisation at the policy level.

Although all investigative powers are available for the purposes of ML, recent legislative amendments, have raised the evidential threshold for obtaining investigative orders for all criminality including ML, creating a significant challenge that is dissuasive to both police and prosecutors. This issue is compounded by restrictions placed on the authority's ability to utilise information held on public registers for evidential purposes.

Overall, while Slovenia has the necessary tools and demonstrates some positive results, deficiencies such as lack of autonomous ML, weak sanctions, and procedural inefficiencies, indicate that effectiveness is achieved to some extent.

Slovenia is rated as having a moderate level of effectiveness for IO.7.

553. Slovenia has established legislative and institutional frameworks that allows for the identification,

investigation and prosecution of ML offences, despite some unfavourable amendments to the criminal legislation in 2024 which have had an impact on all investigations including ML.

554. In 2017, Slovenia was rated as having a moderate level of effectiveness for IO 7, with deficiencies identified including amid others: a lack of systematic parallel financial investigations, uncertainty as to the evidentiary requirements in proving ML and the underlying predicate offence, lack of resources and insufficient expertise on financial crimes.

555. Since then, it was observed that the authorities, are facing certain challenges, particularly in pursuing autonomous ML offences. Nevertheless, there are concrete steps being taken and results achieved which has led to ML investigations, prosecutions and convictions of offenders. A detailed analysis is provided below.

7.1. ML activity identified and investigated

556. In Slovenia, the police, as the responsible investigative authority, undertake pre-investigations at a local, regional, and central level. The National Bureau of Investigation is tasked with identification and pre-investigation of the most complex ML cases stemming from economic crime, corruption and organised crime. Some complex ML cases are also investigated at regional units. The local police units detect and pre-investigate minor ML cases stemming from fraud and online fraud.

557. Initial criminal reports are submitted to the prosecutor (SPO for complex cases and District Prosecutors for others) which is responsible for assessing the case, agreeing and preparing applications to the court for investigative orders. The prosecutor may where it is considered necessary establish and lead a joint investigative team with participants from the police and other competent authorities such as FARS. Upon the motion of the prosecutor, the Investigative judge is tasked with leading judicial investigation. Before initiating a judicial investigation, the judge will need to confirm that there is enough evidence to support the charges. Such decisions are subject to appeal. A number of check and balances available before confirming the charges serve as a gatekeeper for human rights. Nevertheless, the authorities stated that there are instances where such robust procedures are abused by defendants in order to prolong the process. Once the investigation is completed, the case is referred back to prosecutor who will further decide whether to prosecute the case or not.

558. Relevant training and support including upskilling sessions in identifying and conducting ML investigations are provided to the police, SPO and OMLP, with instances of international courses being attended by both prosecutors and the police that seeks to rectify the previously identified lack of expertise in fight against financial crime. Police training includes a centrally managed mandatory national syllabus to which Prosecutor’s actively contribute and includes modules dedicate to ML and asset recovery. Training for Prosecutors and the Judiciary consists of regular topic-based lectures and events, the subjects including ML being addressed regularly. The authorities desire to build their capabilities is further evident in the nascent specialist resource for the identification and tracing of crypto currencies and digital assets that is being developed by the police that includes a central resource that supports local and regional police. This confirms the authorities’ commitment to adapting their investigative tools and expertise to address the evolving challenges posed by digital financial crime.

559. Slovenia seeks to identify and investigate instances of self and third-party ML where predicate offending has been established. Conversely, autonomous ML offences cannot be effectively investigated without the predicate offending being identified and established.

560. ML is primarily identified through parallel financial investigations conducted alongside investigation of predicate offences. Parallel financial investigations are regularly conducted in all

acquisitive crimes, with the aim to identify and trace the proceeds of crime and identify ML offence. ML investigations also originate from the OMLP disseminations, overseas requests and CTRs. The authorities prioritise offences that generate high levels of criminal proceeds, such as corruption, economic and organised crime.

561. The 2025 NRA identifies the highest risks of ML as being associated with economic crime, organized crime, classic property crimes (online frauds and attacks on online system) and corruption, with increases in instances of ML arising from on-line fraud offences. External threats associated with cross border crime and foreign perpetrators were deemed to be of medium risk. Notably the risk assessment identifies self-laundering as the principal type of ML. The risks identified reflect the status of Slovenia as a regional transit state for legitimate and illicit goods, such as illicit drugs and immigration, with internal land borders with four EU states Austria, Croatia, Italy and Hungary, as well as international airports and a containerised seaport.

562. Data supplied for predicate offending during the assessment period (2020-2024) indicates a total of 103 179 acquisitive offences being investigated by police, with the principal offending being theft (79 000) and drugs trafficking (5 887) and human trafficking offences (2 061), with recorded significant instances of all types of fraud (15 000), and bribery and corruption (1 231). The authorities note that between 2023 and 2024 there was an increase in the instances of fraud, in particular on-line fraud (610 cases in 2020 increasing to 2 064 in 2024), which has contributed to the increased number of ML investigations being conducted.

563. During the relevant period the police conducted pre-investigations in relation to ML offences in 378 cases against 934 natural persons and 99 legal persons, representing 2.90% of the reported predicate investigations. There is an increase of the number of pre-investigations in 2024 due to the surge of online frauds, as explained by the authorities. Majority of these cases are initiated as an outcome of the parallel financial investigations carried out within the investigation of predicate crime.

564. The authorities argued that a percentage is 6.8% based upon a number of domestic factors not immediately evident in the data provided. These include instances of multiple offences recorded in single cases and low-level offending typically not subject to ML investigations. Both metrics represent low instances of predicate offending being investigated as ML or with associated offending.

565. Several contributory factors impact on the ratio cited above, such as proportionality where sanctions for predicate offending exceed those for ML, where resourcing is not justified given the potential outcomes of a successful investigation, specifically the likelihood of ML investigations being adopted by Prosecutors for Judicial investigation.

566. The authorities are proficient in engaging with counterparts from other States, in particular regional jurisdictions with whom examples of JITs were established and co-ordinated action undertaken. The authorities' capabilities regarding this aspect of investigations are particularly important given the complexity and nature of the predicate offending from which the ML risk identified in the NRA is derived.

Table 7.1: No of pre-investigations conducted by police

	No. of cases (files)	Natural persons	Legal persons
2020	40	118	17
2021	53	103	22
2022	72	130	18
2023	85	237	24
2024	128	346	18
Total	**378**	**934**	**99**

567. The number of cases that are subsequently adopted for Judicial investigation reflect further attrition. Compared to the 378 police pre-investigation case, the number of Judicial investigations for the same period is 90, with the number of individuals and legal persons being investigated being 1 033 as opposed to 156. The most significant difference is in the number of cases for legal persons that constitute 99 of the police investigations in contrast to the 13 Judicial investigations, equivalent to 13.13% of the pre-trial cases.

Table 7.2: ML Judicial Investigations conducted (State Prosecutor's Office)

	No of cases		No of persons	
	Natural persons	Legal persons	Natural persons	Legal persons
2020	19	1	35	6
2021	17	0	26	0
2022	17	0	26	0
2023	21	5	47	5
2024	8	2	9	2
Total	**82**	**8**	**143**	**13**

568. A number of potential reasons for the discrepancy between pre-trial investigations and judicial investigations have been identified including the time taken to reach decisions, prioritisation of predicate offences, the dismissal of complaints or their non referral due to a lack of evidence. A further factor, based on the discussion during the onsite, is the subjective interpretation of the likelihood that ML prosecutions will result in a conviction and that the conviction will make a difference if a predicate has also been successfully prosecuted.

569. The majority of ML investigations originate from fraud. However, the authorities demonstrated instances of ML investigations linked to other acquisitive predicate offences such as drug trafficking and human trafficking. These results are aligned to some extent with the identified risks, particularly that in the recent period number of ML cases increased due to the increase of the number of fraud offences. Nevertheless, the AT raised concern over the limited number of ML investigation stemming from human trafficking, particularly considering the high volume of investigations and MLA request related to this offence. While the AT acknowledges the authorities' view that lack of cooperation from overseas countries hinders domestic investigation, it notes the lack of proactive approach to address these challenges. In one case study, the authorities engaged with other jurisdictions and utilise a range of investigative techniques to investigate ML and human trafficking. During the searches significant sums of cash were discovered and seized along with corroborating evidence that linked the specific notes to the offending, to different suspects and potential cash smuggling from Taiwan. The cash was subsequent forfeited solely as the proceeds of the human trafficking as the money laundering prosecution was not progressed due to the cross over with the predicate offending and difficulties obtaining evidence from other jurisdictions.

570. There are no statutory prohibitions on the use of the full range of investigative techniques and powers in ML cases, however following a Constitutional court ruling and amendments to Art.156 CPA in 2024, the legal basis for obtaining financial information changed. The amendments introduced stricter requirements for the issuance of judicial orders including a higher evidentiary threshold to suspect that a specific or identifiable person has committed or is committing a criminal offence. The amendments also affected requests for subscriber data, requiring court orders in cases of natural persons, with the authorities having to demonstrate a substantial inference that a criminal offence has or will be committed. In real terms this means that an investigative order is only available in instances where the investigator can already demonstrate high level of suspicion thereby limiting the use of such powers for proactive purposes to identify criminal activity. Given the nature of ML offence, such limitation coupled with high evidentiary threshold for autonomous ML offence hampers the possibility to timely identify ML activities. The authorities have noted that a statistical review conducted by the MoJ following the changes did not indicate increased difficulties, rather a transition to other methods of obtaining financial records. This does not appear to be consistent with the onsite feedback from practitioners, who identified the changes as having a significant impact on their ability to identify and develop predicate and ML investigations.

571. The authorities are proficient in engaging with counterparts from other States, in particular regional jurisdictions with whom examples of JITs were established and co-ordinated action undertaken. The authorities' capabilities regarding this aspect of investigations are particularly important given the complexity and nature of the predicate offending from which the ML risk identified in the NRA is derived.

572. The authorities do not investigate autonomous ML without establishing a predicate offence as they believe it unlikely that the cases will be successfully prosecuted. This belief is supported by the interpretation of ML offence by the Supreme court ruling which found that 'the offence of money laundering cannot exist without the so-called predicate offence. The perpetrator of money laundering cannot, by simultaneously carrying out the acts constituting the elements of the predicate offence, also be laundering money'. These finding were present in the 2017 MER.

573. The authorities clarified that several measures have been undertaken in order to rectify this deficiency. It should be commended that the prosecutors did use their legislative powers (extraordinary remedial measures) to challenge the court's interpretation. Subsequent rulings have sought to clarify these provisions to some extent noting that a final verdict (conviction) in relation to the predicate is not required, nor is the perpetrator's identity, it is sufficient that the objective facts of its commission are established. However, the authorities explained that the evidentiary threshold, as interpreted by the judiciary, is still high in relation to predicate offence to be proven which prevents them from initiating standalone ML case.

574. The requirement to establish the predicate limits the competent authority's ability to disrupt ML activity, and to develop intelligence in relation to ML typologies beyond those linked to parochial offending, and to intercede in cross border money laundering. This deficiency is evident in consideration of typologies such as MVTS and cash smuggling, which is contrary to examples of both being identified within the jurisdiction by the police and Security Services. However, there are instances where the police went beyond the established interpretation of the ML offence by the judiciary (Box 7.1). In this case, the police were able to obtain a further detention to investigate a seizure linked to cross jurisdictional cash couriers even though the requirement of "reasonable ground to suspect" was not met as required by the jurisprudence.

Case Box 7.1. Operation Seizure of 1.8 million EUR

In April 2019 Slovenian authorities stopped a Hungarian registered freight vehicle transporting EUR 1 785 315.00 in cash. The driver and the passenger were unable to explain the origin of the funds, leading to their arrest and seizure of their mobile phones. The seized cash was secured and deposited in a special bank account and an investigation into suspected money laundering was initiated despite the predicate not being identified. The authorities initiated the creation of a JIT with several countries. Three further associated seizures were identified in France and Spain where cash totalling EUR 1 782 000.00 was being transported in vehicles owned or operated by Chinese nationals to Hungary. At the same time, OMLP enquiries further identified cash deposits totalling more than EUR 2 million made by the owner of the vehicle into a business account held in Slovenia that were subsequently transferred to a company in Hong Kong.

Findings of the joint investigation identified links between Hungarian cash couriers and cash deposits by Chinese nationals. The analysis concluded that between 2017 and 2020, between EUR 70–100 million was brought into Hungary from Spain, Italy, France, and the Netherlands. This cash was deposited into company accounts and, in most cases, subsequently transferred to accounts in China, as well as to some EU accounts.

Following the arrest of one of the subjects in Hungary, the police submitted the criminal complaint to the SPO, resulting in the court issuing orders for an investigation into 4 defendants for the offence of money laundering. The SPO filed an indictment and proceeding before the court is on-going.

575. The example demonstrates that it is feasible to initiate an investigation prior to a defined predicate offence being known despite the issues previously identified. The example further reflects the authorities' capabilities in regard to engaging with regional colleagues and their successful use of cross jurisdictional investigative resources.

576. The authorities identify the issues associated with undertaking enquiries overseas and receiving evidence form other jurisdictions as a significant factor in this case that led to delays in the ML investigations.

7.2. Prosecuting and convicting different types of ML activity[24]

577. Slovenia can prosecute self-laundering and third-party ML cases whilst an autonomous offence will only be prosecuted if the predicate offence is established, as explained under the previous core issue.

Case Box 7.2. Abuse of position & Money laundering prosecution 2023

Between 2022 and 2023, the SSPO led a specialist investigative task force consisting of representatives of a number of competent authorities, including the OMLP, in relation to a large-scale pre-trail investigation into criminal offences against the economy. The OMLP analysed sophisticated financial schemes and contributed with comprehensive reports to the investigation, helping to uncover a ML network that operated transnationally in the region. The suspected offending crossed multiple jurisdictions, necessitating the establishment of a JIT that facilitated co-ordinated action including property searches.

In 2023, indictments were filed, charging 3 individuals with offences of abusing a position of trust in economic

24 See *Methodology, IO.7, Note to Assessors 2 and related footnotes*

activity, tax evasion and money laundering. The indictment alleged that the principal defendant operated a system of fictitious business transactions between 2017 and 2023, laundering large amounts of money together with the co-defendants. Among other acts, he laundered approximately EUR 3.2 million between 2017 and 2023 for three clients in Slovenia. He committed the offence of money laundering using at least five shell companies. He ensured the transfer of these companies to foreign nationals, who were formally recorded as the directors and owners.

Seven plea agreements were agreed in 2024 that resulted in convictions for money laundering, abuse of position and tax evasion. The court imposed one custodial sentence of 2 ½ years, as well as suspended sentences and community service, fines up to EUR 720 000 and restitution up to EUR 1 195 000.

578. Prosecutors are required to prosecute without unnecessary delay, where there is a well-founded suspicion that a criminal offence has occurred. Cases filed by the state prosecutors may be prosecuted in any of the 11 District courts, those filed by the SSPO are referred to in one of the four designated specialist financial crime District courts located at the seat of the 4 higher courts (Ljubljana, Maribor, Celje, Koper). Judges assigned to hear the cases have received specialist training to ensure the efficient progression of the matter. Revised standards and procedures were introduced in 2024 that imposed improved case progression and to ensure timely resolutions.

579. Slovenia's legal framework provides multiple opportunities for an individual to challenge or appeal prosecutorial and judicial decisions at various stages of the investigation and prosecution. Whilst offering a safeguard for individuals, the potential delays resulting from these appeals impact on the timely conclusion of prosecutions and adversely impact on resources and create trial backlogs. Further delays arise from general resourcing issues and unsuitable or outdated court facilities, which have led to instances of private venues having to be used with the associated security and practical issues impacting on the efficiency of the court. The authorities reported that some measures at the court level have been taken in order to resolve older criminal cases and meetings have been held with relevant courts and the Judicial Council to discuss the problems and possible solutions. While this is assessed as a positive step, the effectiveness of such measures are yet to be seen.

580. During the assessment period the data provided shows 151 prosecutions were undertaken against 236 legal and natural people, which resulted in 67 convictions in 56 of the cases for ML offences. There is no breakdown of different types of ML offences, but the majority of them are third party and self-laundering.

Table 7.3: number of ML cases prosecuted, and convictions achieved

Year	Prosecutions *cases (persons)*	Convictions *cases (persons)*	% of prosecutions leading to conviction *cases (persons)*
2020	21 (39)	11 (14)	52 (36)
2021	25 (42)	13 (14)	52 (33)
2022	26 (46)	11 (12)	42 (26)
2023	33 (49)	9 (11)	27 (22)
2024	46 (60)	12 (16)	26 (27)
Total	**151 (236)**	**56 (67)**	**37 (28)**

581. The ratio between successful convictions and prosecutions has decreased over the assessment period with a decline from 52% in 2020 to 26% in 2024. Similarly, the percentage of individuals convicted declined from 36% to 27%. The AT identified that undue delays in trials before the court and court backlogs are contributing factors.

582. The data relating to pre-trial police and Judicial ML investigations provides wider context. During the period, the number of pre-trial investigations compared to the prosecutions suggest that 39.9% of cases under police pre-investigation resulted in prosecutions, leading to convictions in 14% of cases, while the number of convictions compared to cases of Judicial investigations (Tables 7.1, 7.2 and 7.3) equalled 62%. These figures reflect the effect of the review process undertaken by Prosecutors on receipt of a referral and a high level of attrition between pre-investigation and Judicial investigation The variance in these figures and the process of investigations resulting in no further action is low.

583. Although legal persons are frequently used to facilitate money laundering activities, they are rarely investigated or prosecuted for the offence of money laundering. According to the authorities, this is mainly because such entities are often shell companies that cease to exist by the time proceedings are initiated. However, the AT came across several instances where legal persons, that were not shell companies, were not considered for ML investigations, which raises concerns. The authorities were not able to explain reasons behind such decisions.

584. There is insufficient data on the profile of ML cases that led to prosecutions and/or convictions. However, the cases reviewed indicate a consistent trend, with most being linked to fraud, mirroring the broader pattern observed in ML investigations. The AT concludes that these results are to some extent in line with country's risk profile.

7.3. Effectiveness, proportionality and dissuasiveness of sanctions

585. The sanctions applied to ML convictions remain insufficient and cannot be considered either dissuasive or effective.

586. During the assessment period, 44 custodial sentences were imposed for periods ranging between one and thirty months, of which 30 were suspended. Fines were imposed ranging from EUR 658 to EUR 100 000. There is a reliance on asset recovery as a means of resolving cases with confiscation of assets against legal persons and forfeiture of objects being applied in up to 125 instances, this reliance is not an acceptable substitute for effective sanctions. The number of sanctions recorded exceeds that of the number of outcomes. This anomaly may be due to different types of sanctions and custodial sentences being applied together against an offender, or that sentencing from an earlier period has been captured in the sentencing data. The use of multiple sanctions, such as suspended sentences and imposition of a fine, may be a rationale for not imposing custodial sentences, reducing the dissuasiveness of sanctions.

587. The low level of sanctions may be explained by the parallel nature of prosecutions, where sanctions are simultaneously applied for both the predicate and the ML. There is a clear rationale for this approach, ensuring dual sentencing is proportionate, and agreements ensure timely outcomes. A resource intensive trial can be avoided, while the defendant can expect a more lenient sentence and quicker resolution to the proceedings, which is consistent with the nature of domestic criminality where ML is an adjunct to the predicate offence, which will be subject to higher sanctions on conviction. It is also possible that the judicial view of ML as an accessory to the predicate impacts upon the priority and seriousness with which the court approaches ML matters and any sentencing following conviction.

588. A consequence of the low level of sanctions is the extent to which the investigation and prosecution of ML is incentivised and prioritised, given the general pressures on the police, prosecutors, and Investigative Judges, who are required to prioritise predicate offending over ML. This combined with the reluctance to prosecute autonomous ML supresses the volume of ML cases; in doing so it restricts the development of specialist skills amongst Investigators and prosecutors.

589. The ineffective nature of sanctions against both natural and legal persons was highlighted in the previous MER, the absence of any steps to resolve this matter implies, with other areas of continuing deficiencies, a low priority being given to an effective ML regime.

7.4. Use of alternative measures

590. In Slovenia, when ML convictions are not feasible for justifiable reasons, the authorities pursue predicate offence and apply non-conviction based confiscation.

591. The non-conviction-based provisions of the Act on the Confiscation of Assets of Illegal Origins (ZOPNI) are considered by the authorities to be an alternative means by which autonomous ML offences can be resolved in the absence of a predicate conviction. This legislation includes provisions for investigative orders comparable to those under the criminal provisions and allows for a 'financial investigation' distinct from parallel investigations. It is not a substitute or an effective alternative to prosecutions.

592. Data provided by the authorities and the onsite narrative indicates that the use of ZOPNI is perceived by the authorities as an alternative to autonomous prosecutions. But its use in relation to ML appears to be low with 2 recorded outcomes totalling EUR 242 380. These figures do not include the case of a Slovenian Syrian national, who was investigated for drugs offences but not prosecuted, where ZOPNI was used to order the forfeiture of EUR 219 000 by means of charges placed on property held by the subject's company. The effectiveness of ZOPNI as an alternative measure is being further challenged as a recent court ruling required the assets being recovered to have 'undeniably originated from the commission of a criminal offence' thereby potentially requiring the prosecutor to be able to evidence the predicate(s) and trace the proceeds.

Chapter 8. Asset Recovery

The relevant Immediate Outcomes considered and assessed in this chapter is IO.8. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 32 and elements of R. 15, 30, 31, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) The competent authorities (police and prosecutors) prioritise asset recovery through their own policies, nevertheless these efforts are not sufficiently supported at a Ministerial level leading to the lack of sufficient resourcing. There is no comprehensive periodic review of asset recovery regime or central data on which a review could be based, that would identify deficiencies and map crime trends. Cooperation and information exchange in asset recovery matters between competent authorities work very well in practice.

b) Asset tracing and recovery are a mandatory element to all investigations conducted by the police and prosecutors in regard to acquisitive criminality, within the scope of parallel financial investigations. The range of investigative powers are available to them, however 2024 legislative amendments regarding banking data pose a challenge when identifying and tracing certain assets.

c) Competent authorities make frequent use of provisional measures to freeze and seize criminal property and property of corresponding value. A commendable value of criminal property has been seized during the review period. However, some attrition remains between police proposals and the orders ultimately issued by courts, reflecting the higher evidentiary threshold that prosecutors are required to meet when submitting motions for court-ordered measures, and longstanding barriers to issuing freezing orders in the absence of a court order.

d) Responsibility for managing seized or frozen property is allocated to a number of authorities based on their competencies. Each is tasked with the storage, maintenance, and ultimately realisation based upon the requirements of the court's order, regarding which they maintain their own records. Pre-confiscation sale of seized property has been applied in some instances to prevent the dissipation of assets. However, the absence of centralised records and data pertaining to assets frozen, seized and confiscated remains a deficiency.

e) The effectiveness of the confiscation of criminal property and property of corresponding value is undermined by the absence of effective records and data, although some data is held by individual authorities. Legislative provisions include both conviction based and non-conviction-based recovery. The competent authorities have demonstrated the application of each of the asset recovery methods available to them. However, the extent to which the instrument of NCBC is used is limited.

f) Victims are able to seek recovery of funds within the criminal proceeding by demonstrating proprietorial rights, and victim compensation takes priority over confiscation. This is consistent practice across all cases. However, there is a vulnerability where corporate entities owned or controlled by offenders may be treated as victims, enabling offenders to recover proceeds through their companies and thereby undermining confiscation outcomes.

g) The identification and seizure of undeclared or falsely declared cash remain limited, despite indication of the significant volumes of cash entering or transiting through the jurisdiction. Only one detected case of undeclared cash resulted in a criminal investigation for ML offences during the review period. In addition, sanctions imposed for failures to declare cash are not effective, proportionate and dissuasive.

Key Recommended Actions (KRA)

a) Slovenia should prioritise its recent efforts to establish a dedicated asset management office to ensure the effective oversight, management and preservation of frozen and seized assets, and to support the timely enforcement of seizure and confiscation orders.

b) The competent authorities should identify and address the key impediments to the effective use of non-conviction-based confiscation and extended confiscation to ensure it can be applied effectively in practice.

c) Slovenia should address the issues of the proceeds of criminality from being returned to offenders; specifically, to prevent corporate entities or other legal persons from being abused to frustrate confiscation through offenders claiming compensation.

Other Recommended Actions

a) Slovenia should conduct periodic reviews of their confiscation regime and adopt high level policy which would address overarching issues impeding effective asset recovery.

b) The authorities should keep comprehensive record of criminal property and property of corresponding value subject to seizure, freezing or confiscation, including breakdown by predicate offences.

c) FARS should conduct a review with key stakeholders of the effectiveness of the cross-border cash and BNI declaration system and the provisions for the detection and interdictions of cross border transportation of cash. This should result in effective detection of undeclared cash and application of effective and proportionate sanctions.

Overall Conclusions on IO.8

The competent authorities demonstrate a commitment to asset recovery and victim compensation using both conviction-based and non-conviction-based confiscation. Parallel financial investigations are a mandatory component of all criminal investigations, and the authorities have provided examples of significant amounts of assets frozen or seized, including through cross-border cooperation and the recovery of crypto-assets which have been assessed as important elements.

Notwithstanding these positive elements, several deficiencies remain. A central register of assets subject to freezing, seizure or confiscation has not been established since the previous MER. This limits the authorities' ability to manage assets effectively, prevent devaluation, follow the trends and apply measures where risks emerge. Further it limits the authorities ability to analyse and understand the extent to which confiscation is being effectively applied and managed. There is general lack of comprehensive statistics. Legislative changes to evidentiary thresholds for obtaining court-ordered measures, compounded by restrictions on evidential access to some databases, and restrictions to freezing property in the absence of a court order continue to affect the effectiveness of asset recovery. In practice, there appear to be limited mechanisms to ensure the effective recovery of confiscated assets, and issues were identified regarding the legal status of corporate entities following confiscation, which may allow offenders to reclaim criminal property.

While Slovenia operates a cash declaration system broadly in line with EU requirements, enforcement related to cash smuggling remains challenging and is not effective. The impact of these shortcomings is heightened by the fact that several of them were identified in the previous MER and remain unaddressed, indicating that asset recovery has yet to be fully prioritised at the strategic or policy level.

Slovenia is rated as having a moderate level of effectiveness for IO.8.

8.1. Prioritisation of asset recovery as a policy objective and using effective agency structures and cooperation frameworks

8.1.1 Prioritising asset recovery as a policy objective

593. The asset recovery regime has been prioritised by the competent authorities, with policy issued by the police and Prosecutors at the highest level to ensure a consistent approach to asset tracing and recovery. Supreme State Prosecutor's issued 2024 Law Enforcement Policy obliging prosecutors to give priority to seizure of assets in order to secure confiscation and engage in the early stage of the pre-trail proceedings by providing to police guidelines including those related to tracing and seizing of assets. Ministry of interior issued policy addressing the issue of tracing and seizing of assets as priority. These documents emphasise that financial investigations are mandatory and should be carried out as early as possible.

594. Guidance has been produced by the police and SPO to support and prioritise asset tracing and recovery during the investigation stage of the proceedings, however similar guidance is not provided to Investigative and Trial Judges.

595. Furthermore, priority given to the confiscation regime has not been sufficiently supported at the higher level which has contributed to persistent and long running deficiencies in the regime.

8.1.2 Periodic review of asset recovery regime

596. No central strategy or review process of the asset recovery regime has been carried out. This is reflected in the inadequate institutional capacity to deal with asset recovery issues. Resourcing at all levels and in all competent authorities is an issue, that was raised during the onsite, in particular amongst prosecutors and the courts. An example of these limitations is the resources dedicated within the SPO to the implementation and use of ZOPNI, which currently has one dedicated resource to support all ZOPNI cases. This has led to a low level of engagement with the legislation in the wider SPO. There is a systemic issue of the legislative barriers to obtain court orders for some investigative measures (see IO 7), no action has been undertaken at the highest political level to analyse and address these practical issues. This is

despite an impact assessment conducted by the Police following the Constitutional court's ruling that identified the likely negative impact on investigations.

597. In addition, while seizure and confiscation results have been analysed within the 2025 NRA to some extent, none of the identified problems were reflected and captured by the 2025 NRA Action Plan, which raises concerns.

8.1.3 Effective agency structures and cooperation frameworks

598. The competent authorities effectively co-operate in order to prioritise asset recovery, in particular the police, and the SPO, who are responsible for ensuring that the parallel investigation is conducted in a timely and effective manner and appropriate orders obtained to secure assets. Both authorities have developed specialist teams responsible for complex economic crime, along with specialist crypto resources. Cooperation and information exchange between these authorities work very well in practice.

8.2. Identifying and tracing criminal property and property of corresponding value

599. The authorities are able to use the full range of investigative powers when identifying and tracing criminal property and property of corresponding value and there are no barriers preventing the use of evidence in assets recovery. There are legislative provisions for both non-conviction and conviction-based recovery against legal and natural persons, with provisions for both extended confiscation as well as the seizure and confiscation of assets of corresponding value.

600. The police undertake regular training and upskilling courses to enhance their capabilities to trace assets including virtual assets.

601. Parallel financial investigations are mandatory and conducted by police under the supervision of prosecutor. They are always conducted alongside investigation of a predicate offence with the main purpose to identify and seize assets subject to confiscation. There are no legislative constraints on the use of investigative orders in the tracing of assets associated with a criminal investigation, nor are there any restrictions on the use of material obtained where the primary purposes of an enquiry were the criminal offence. However, the effectiveness of the parallel financial investigation is impacted by the issues noted in IO.7 of the increased evidential threshold for obtaining investigative orders (information on bank accounts) and restriction on utilising some existing data bases. The exception being publicly held records relating to corporate entities. The impact of these limitations is particularly relevant in instances where there is a risk of concealment or dissipation at an early stage of the pre-investigation.

602. The authorities have demonstrated an ability to engage with other jurisdictions, to obtain intelligence via the FIU, gather evidence and form JITs to trace criminal assets abroad. The authorities regularly participate in JITs which has been proven to contribute to the effective identification and tracing of assets. These JITs included EU and non-EU member states. During the onsite examples of cases provided by the authorities identified instances where assets had been identified in other jurisdictions (see IO.2).

Case Box 8.1. Overseas crypto asset seizure

In 2016 a JIT at the national level was established for the purpose of seizing of virtual currency Bitcoin that was believed to be linked to alleged drugs and money laundering offences. Within the JIT information was exchanged with the FIUs of Luxembourg, Saint Vincent and the Grenadines, the Netherlands, and Lithuania. During house searches, electronic devices were seized and the data stored on them was analysed. It was established that the suspects held Bitcoin in foreign accounts (at Bitstamp in Luxembourg). The judicial authorities in Luxembourg executed the Slovenian court order from 2017 (which became final in 2020), seized the Bitcoins, and acting upon the Slovenian request converted them into euros (EUR) to preserve the value of seized assets.

The conversion of the Bitcoin to fiat was undertaken by consent to preserve the value and supported by a court order for the sale of assets that had not previously been used for crypto assets. The court was further required to consider the most appropriate and effective means of realising the Bitcoin, which gain required an innovative approach to be adopted.

Following the conviction in 2019 of the offenders a confiscation order for EUR 138 869.72 was issued by the court, this being in part the fiat value of the converted Bitcoin.

Source: SPO Book of cases – No.11

8.3. Freezing and/or seizing criminal property and property of corresponding value

Freezing and/or seizing criminal property and property of corresponding value

603. The prosecutors, upon the motion of the police, can request the court to freeze and seize assets subject to confiscation. This is systematically done in all instances related to predicate offences, including as a result of financial investigations. Nevertheless, in ML cases (particularly standalone) due to the high evidentiary threshold required for predicate criminality, these measures cannot be swiftly undertaken. The prosecutor shall provide enough evidence to support the existence of predicate criminality in order to substantiate suspicion for ML which is further necessary for the court to issue the order and seize funds.

604. As noted previously, there is no centralised comprehensive record of seized criminal property and property of corresponding value, the authorities have however provided SPO data compiled by the Competence and Information Centre (CIC) regarding the rates of referrals, seizure and orders obtained, as well as a breakdown of assets frozen and linked criminality. The CIC is required to record and retain SPO performance data, including that relating to organisational freezing and temporary seizing of assets. The referrals, seizure and orders obtained data set reproduce in Table 3.1 provides an indication of performance but is caveated as potentially being incomplete for a number of systematic reasons.

605. The data demonstrates an upward trend in the instances of referrals submitted to the SPO by the police, with corresponding increases in the numbers of applications to the court and freezing orders obtained during the assessment period. The figures further illustrate a general upward trend in relation to the percentage of successful applications made by the SPO. The data is derived from the 'Joint annual reports of the prosecution offices', which also reports that as of the 31st of December 2024 a total of 381 freezing orders were in place over assets with an estimated value of EUR 232 972 949. The amount seized and the positive trends in referrals and orders is commendable.

Table 8.1. Number of seizure orders

Year	No. of police *initiatives* to secure assets for confiscation	No. of *proposals* made by prosecutors for seizing assets	No. of seizing orders obtained	% of successful applications to seize	Value of assets under provisional seizure (€) *
2020	155	72	55	76.4	224 153 330
2021	149	61	44	72.1	50 029 205
2022	204	132	115	87.1	108 090 254
2023	224	134	125	93.3	290 875 312
2024	259	185	167	90.3	232 972 949
Total	**991**	**584**	**506**	**88.6**	**906 121 050**

606. There is however a question as to the reason for the disparity between police initiatives and prosecutor proposals, with 407 initiatives not being progressed (see table 8.1).

607. The data supplied indicates a significant discrepancy between the number of police initiatives and the number of prosecutor’s proposals, with 407 initiatives not being progressed. The difference between these figures can be explained by a combination of factors, including the requirement to initiate parallel investigations in all matters irrespective of assets or losses being identified, the requirement for proposals to demonstrate reasonable grounds for suspicion for the predicate offence, and the criminal offence of money laundering, as well as the risk that the suspect or a third party will dispose of the property in such a way that it will no longer be possible to confiscate the proceeds of crime or assets.

608. Conversely, the rate of conversion of proposals to orders is significantly better, this could be interpreted as being demonstrative of prosecutor’s applying a proportionate and subjective review of evidence or alternatively may indicate a risk adverse approach to applications that seek only to advance those with a probability of being granted.

609. The data also suggests that there is an issue with the timely progression of these matters as a total of 381 orders, identified in the annual report, remained in place at the end of 2024, compared to the 506 that were obtained during the five-year assessment period. This means that 75.3% of the orders obtained during the five-year period remain extant, with resolutions in only 24.7% of cases. This is indicative of delays in proceeding due to challenges, court availability or realisation of assets following a final ruling in the matter.

Table 8.2. No of seizure orders

Year	Real Estate No. measures ordered	Movable Property No. measures ordered	Money No. measures ordered	Securities No. measures ordered	Other No. measures ordered	Total No. measures ordered
2020	27	22	60	6	7	122
2021	28	9	53	3	10	103
2022	37	11	69	2	5	124
2023	27	5	102	2	8	144
2024	24	12	144	3	6	189
Total	**143**	**59**	**428**	**16**	**36**	**682**

Table 8.3. Types of seized assets by value in EUR

Year	Real Estate value (€) ordered.	Movable Property value (€) ordered.	Money value (€) ordered.	Securities value (€) ordered.	Other value (€) ordered.	Total value (€) ordered
2020	3 923 687	596 737	16 848 475	9 168 789	355 015	30 892 703
2021	3 674 256	195 556	9 498 523	5 260 032	1 070 582	19 698 949
2022	6 372 733	307 611	27 766 406	2 273 598	720 549	37 440 897
2023	6 049 564	89 251	194 402 023	2 273 598	4 303 262	207 117 698
2024	4 402 462	542 998	34 822 318	877 098	9 202 387	49 847 263
Total	24 422 702	1 732 153	283 337 745	19 853 115	15 651 795	344 997 510

610. The authorities are able to seize different type of property as it can be seen from tables 8.2 and 8.3. The types and nature of property subject to freezing measures ordered by the court, indicate that during the assessment period measures were applied in 682 instances for a combined value of EUR 344 997 510. Of the property types identified, 62.7% of measures were against money, and 21% in relation to real estate. The records also demonstrate the frequency and value of property by the nature of the criminality, with fraud being the most significant, accounting for 45.3% of all orders and 59.4% of the overall value. The fraud related instances are marked by a particular increase in 2023 and 2024. The volume of Fraud related activity is consistent with the NRA and overall risk understanding of the authorities.

Table 8.4. No. of freezing measures ordered by predicate offence 2020 -2024

Offence type	No of measures ordered	Value of property (€)
Abuse of position or trust in economic activities	104	9 7047 230
Causing bankruptcy through dishonest management	1	108 000
Corruption and bribery	13	1 458 015
Damage to creditors	14	4 512 679
Deception in obtaining and using a loan or benefit	3	118 250
Embezzlement and improper use of other people's property	38	2 515 322
Forgery	36	4 089 763
Fraud	309	205 025 581
Illicit arms trafficking	7	635 876
Illicit trafficking in narcotic drugs and psychotropic substances	43	2 544 153
Robbery or theft	28	5 909 640
Sexual exploitation, including sexual exploitation of children	13	8 634 951
Smuggling (including in relation to customs and excise duties and taxes)	1	7 500
Tax crimes (related to direct taxes and indirect taxes)	66	11 919 310
Trafficking in human beings and migrant smuggling	6	471 240

Source: Slovenian authorities

611. These figures are helpful in understanding the frequency of different property types being frozen and the associated criminality. The value provided is given for the property not the criminal benefit determined, which is est. EUR 35 million less. There is an inconsistency between the different data sets which suggests a need for caution as they are significantly higher than those provided elsewhere. This can be explained by instances of the Investigative Judge or Trial Judge seeking or imposing measures separate to the SPO, assets subject to alternative recovery action, duplication of one person across multiple offences, or activity by other competent authorities not effectively captured in the data sets.

612. As noted previously, the ability of the police and prosecutors to act immediately or in a timely manner is hampered by the increased evidential threshold for obtaining banking material, and the

restrictions on the use of some of the existing data bases which is particularly detrimental for standalone ML cases if not mitigated by active judicial co-operation.

613. The OMLP has the order suspension of transaction where there is a suspicion of money laundering or terrorist financing When such a suspension is ordered, the APML must notify other competent authorities so they can take appropriate measures, such as freezing or seizing assets.

614. During the onsite it was noted by both police and prosecutors that a particular issue is their ability to effectively respond in instances where the FIU has imposed an initial 72 hr freeze on assets to enable initial enquiries. There are however examples of both domestic and international cases where the police/prosecutors were able to act immediately. The following case demonstrates commendable efforts of the authorities, such as effective early FIU intervention, timely judicial action, and constructive cross-border cooperation, resulting in the recovery of stolen assets for the victim.

Case Box 8.2

The case originated from an FIU notification to the police, indicating suspicion that the director of a Slovenian company had laundered EUR 25 500 obtained through an online fraud against a Croatian company. Documentation from Croatia confirmed the predicate offence and traced the funds to a Slovenian bank account holding approximately EUR 17 000.

Acting on the FIU's order, the bank temporarily suspended all transactions. Following the prosecutor's request, the District Court in Ljubljana issued a freezing order for EUR 25 500 and transferred the funds to a judicial deposit account. Evidence found during a search suggested that the suspect intended to dispose of the remaining funds.

Upon the Croatian company's request, the prosecution successfully moved for the restitution of the frozen assets, as they clearly belonged to the victim and were no longer required as evidence. The court lifted the freezing order, and the funds were returned to the injured party. An indictment was subsequently filed, and proceedings are ongoing.

Source: VDT Book of cases – ODTLJ14

8.4. Managing frozen or seized property to preserve its value

615. The management of frozen, seized or confiscated assets, including their realisation is the responsibility of the appropriate competent authorities, who are required to execute the court's order in regard to their competency. In March 2025, this multi-agency approach manifested in 18 properties valued at EUR 1 229 759.00 being managed by the Ministry of Public Administration, a 100% shareholding in one corporate entity managed by the Slovenian Sovereign Holding d.d. (SDH d.d.) - and 8 vehicles held by FARS.

616. This multi-agency approach means that multiple authorities may be responsible for executing a single confiscation order. This approach does in theory ensure that management and recovery is undertaken by the most specialist teams, however the extent to which this function is appropriately resourced within each authority is unclear and at least one does not keep any relevant records. The siloing of responsibilities and absence of a co-ordinated approach constrains the effective enforcement and management of the overall order.

617. The authorities are not able to provide reliable consolidated data due to the absence of a central record. This issue was identified in the previous MER, and is an issue recognised by the authorities during the on-site. However, there have been no substantive steps taken to address the issue. The reason for this may be a matter of prioritisation or resourcing, however it remains and are requiring improvement. The current system is based upon each responsible authority in isolation creating and retaining their own records with no means of cross referencing or external review. As such, it is not possible for the authorities to access the effectiveness of the regime, or to ensure that the court orders are executed in their entirety and in a timely manner.

618. The Authorities are able to sell or dispose of assets subject to temporary seizure in instances where the market value may decrease over time, or whose continued storage is associated with disproportionate costs given the potential duration of proceedings, Safeguards exist to ensure that the beneficial owner of the property is consulted and is able to make appropriate representations to the court. In relation to real property, the authorities are required to ensure third party interests are protected and any maintenance costs are met. The AT have however not been provided with any examples to demonstrate the effectiveness or frequency of such actions.

8.5. Confiscating and enforcing confiscation orders

8.5.1 Criminal property and property of corresponding value located domestically

619. As indicated above, the authorities are able to confiscate criminal property and property of corresponding value through conviction and non-conviction-based confiscation, with the latter being rarely used.

620. There is a lack of statistical data which hampers the ability to assess the overall level of confiscation in Slovenia. When it comes to confiscation there are even no estimation on the amount of confiscated property, but authorities were able to provide case examples of successful confiscations.

621. Nevertheless, the SPO produced some statistics, which relates to the number of confiscation orders obtained including those against third parties. The figures with minor variations in 2021 and 2022 are comparatively consistent amounting to 318 orders over the assessment period. The increased numbers in 2021 and 2022 were not maintained and may have been associated with a particular case or other short term anomalous factors, such as the impact of covid-19 in 2020 that restricted court proceedings to urgent cases only and a subsequent peak in confiscations once restrictions were lifted.

622. The actual volume of confiscations is low in the context of the volume of acquisitive crime being investigated, and figures pertaining to seizure and freezing orders for the same period. This discrepancy may be explained by the use of alternative means of restitution (returning the assets to the victims), delays in the prosecutorial process, case closures due to evidential reasons, or ineffective data collection. This data is also specific to those areas for which the SPO is competent, and as such may not represent the full extent of confiscation. It is also relevant to note that the data set does not include the value of orders, which may be due to the absent of a central record of assets subject to freezing or confiscation.

Table 8.5. No. of Confiscation Orders

Year	No. of confiscations	No. of confiscation against third parties
2020	55	4
2021	76	2
2022	65	1

2023	56	4
2024	53	2
Total	**305**	**13**

Source: Slovenian authorities

623. There are limited sanctions available to the court post-conviction to enforce confiscation orders, although the courts may impose a general sanction for failing to comply. This deficiency does not appear to be matter of concern to the authorities, which may reflect a focus at confiscation on the assets already identified. The ability of the courts to impose sanctions is also significantly restricted by the dispersal of asset realisation between the responsible authorities in accordance with the courts order.

624. The absence of data prevents the effectiveness of the enforcement being accessed; however, the issues identified regarding the management of assets and the ability of the court to both check if orders have been fully executed or top apply sanctions indicate that the enforcement of orders is not effective.

625. The investigative powers for non-conviction-based asset recovery provided by ZOPNI mirror criminal investigation powers. The use of ZOPNI remains low, however there is a clear desire by police and prosecutors to effectively utilise these recovery powers. They are aware and see the potential benefits of such regime which if effectively applied would bring added value in the deprivation of criminal property. It is evident through the presentation of the cases that there is specialist knowledge and enthusiasm amongst the dedicate resource, and prosecutors are being upskilled for the proper application of these powers. Nevertheless, there are certain challenges in the system preventing them to effectively apply NCBC.

626. Data provided by the authorities and the onsite narrative indicates that the use of ZOPNI has not been extensively used with two recorded cases totalling EUR 242 380. In these two cases, the authorities, due to the high evidentiary threshold could not prove ML and applied NCBC in order to deprive criminal property. In one additional case, a Slovenian Syrian national was investigated for drugs offences but not prosecuted. The authorities applied NCBC provisions to order the forfeiture of EUR 219 000 by means of charges placed on property held by the subject's company. The effective implementation of NCBC is being further challenged as a recent court ruling required the assets being recovered to have 'undeniably originated from the commission of a criminal offence' thereby potentially requiring the prosecutor to be able to evidence the predicate(s) and trace the proceeds, which raises concern.

8.5.2 Criminal property and property of corresponding value located abroad

627. There is no precise information provided by the authorities on the number or frequency of overseas confiscations or the enforcement of orders in other jurisdictions. As such, a detailed assessment of the effectiveness of oversea recoveries is not possible. The authorities have provided examples of cases where assets held overseas derived from criminality including drugs offences, fraud and money laundering were seized and subsequently made subject of a confiscation order. The examples demonstrate that the authorities are able to and have sought to recover assets from other jurisdictions, however it remains unclear if these examples are representative of a high number of cases or are unique.

8.6. Returning confiscated property to victims

628. In Slovenia, the victims are prioritised by competent authorities. However, no records are kept relating to the value or instances of property being returned to victims, it is therefore not possible to effectively assess the extent that this is done in a timely and effective manner.

629. Victims may, however, seek to recover their property prior to a conviction being obtained, where a proprietary interest can be demonstrated by the victim. the Prosecutor may seek the return of the property directly, thereby minimising the distress to victims and ensuring a timely resolution. During the onsite it was apparent that where possible Prosecutors consider this an effective and common approach to recovering property, which also negated the need to seek confiscation. It is unfortunately not possible to quantify the instances where this approach has been used during the assessment period.

630. Consideration of the means by which victims can recover the property has however resulted in an issue being identified. Currently there are no provisions to prevent an offender, who is a shareholder of a corporate entity they used for criminality, from asserting their victim rights to property recovered as a result of a confiscation order against the corporate. This creates a significant weakness in the asset recovery regime, which if exploited by criminals would negate the effectiveness of the regime. This issue is known to the authorities but has yet to be addressed. In one of the cases presented it was evident that companies were used in the criminality scheme and owned by the offenders. As a result of criminal proceeding, these companies were compensated as victims and the risk remains that the funds paid to them will be recovered by the perpetrators.

8.7. Identifying and confiscating falsely or undeclared currency/BNIs or those related to ML/TF or predicate offences

8.7.1 Identifying and seizing non-declared or falsely declared cross border movements of currency and BNI

631. Slovenia has land borders with Austria, Croatia, Hungary, and Italy, as well as international (non-EU) entry points in the form of Ljubljana, Maribor and Portoroz airports and the containerised Port of Koper. As an EU member state, Slovenia applies the relevant EU Regulations in relation to cross border cash and BNI declarations for values over EUR 10 000 when cash is entering or leaving union. The same threshold applies when cash is carried through the EU member states, yet in these circumstances the disclosure system is applied. The system is administered by FARS, which is responsible for receiving and collating declarations, as well as seizing cash and BNI in instances of false or incorrect declarations.

632. At the port and airports there is clear signage that cash entering or leaving EU must be declared. The local custom offices are located at these entry points. Conversely, customs checks of cash and BNI movements within the EU are primarily conducted by mobile units, which are also tasked to respond to police detections if no criminality is suspected. Cash control functions may also be conducted by customs officers in the clearance departments located at air and seaports, as well as at postal facilities.

633. The mobile units are a limited general resource tasked with a range of FARS roles. There are no additional specialist cash detection resources. None of the authorities provided information on the specific instructions requiring them or guiding them to detect undeclared and falsely declared cash. FARS does have Guidelines for the implementation of supervision under AML law which provides for certain general procedures to be applied according to the legislation for both EU internal and external borders. The issue of lack of resources and equipment to detect cash raises concern given the examples of the cash detected and used in some criminal cases.

634. Once detected, undeclared and falsely declared cash or BNIs may be held for an initial period of up to 30 days, which can be extended to 60 where appropriate to do so. The FARS guidance includes post seizure procedures to ensure consistency including cross organisational and legal provisions that include alternative measures including tax enforcement provisions in instances of outstanding tax debts. Information relating to declarations is available to the FIU via the accessible Customs Information System.

635. Data provided by the authorities demonstrates comparatively low numbers of declarations, and correspondingly low instances of incorrect, false or no declaration of cash and BNIs. Between 2020 and 2024 there were 343 declarations (Table 8.6) in relation to EUR 17 030 051, and 9 instances of non-declaration totalling EUR 220 374, the were no instances of false declarations. During the period instances of non-declaration resulted in 9 instances of misdemeanour sanctions resulting in an average fine of EUR 800 and 1 case of the seizure of EUR 116 510 referred to the police. The status or outcome of this case is not known.

636. Despite an increase in the FARs cash control exercises from 117 in 2023 to 603 in 2024, the latter period resulting in all of the reported detections, the rates of detection remain low and have only resulted in a single case of suspected criminality that is inconsistent with the wider experience presented by the police during the onsite and in the case studies.

Table 8.6 No of declarations or disclosures

	Incoming			Outgoing		
	Cash	BNI	Volume in EUR	Cash	BNI	Volume in EUR
2020	17		1 036 580	34		640 836
2021	15		577 352	31		946 940
2022	37		4 178 224	20	3	1 810 797
2023	42	5	1 872 729	32	3	1 030 674
2024	86	3	3 160 587	29		1 775 332

8.7.2 Confiscation of currency or BNI related to ML/TF or predicate offences

637. FARS have reported 1 instance of a suspected criminal detections of cash that occurred in 2024. As noted above the police cited several instances of cash detentions and seizures within the jurisdiction, and from Slovenian residents or registered vehicles in other member states. As such, it is unclear why FARS are only able to demonstrate limited effectiveness of the controls. The absence of a clear assessment relating to cash movements was mirrored by the FIU, who through consideration of CTRs did note significant cash deposits into Slovenian financial institutions that originated in other states including non-EU jurisdictions. The reason for this deficiency may be the priority given to cross-border cash and BNI movements by the authorities, and a reliance on internal EU controls.

638. In those instances, presented by the police, officers were able to seize the cash for a period of 72 hrs, to conduct initial enquiries. However, a concern raised by the authorities in relation to the effectiveness of the seizure provisions was the restrictions placed on investigative orders previously mentioned, which create significant barriers to obtaining sufficient evidence to seek an extension to the seizure from the court.

8.7.3 Sanctions

639. In instances of incorrect declarations FARs adopt an escalatory approach they describe as 'minor offence proceedings or misdemeanours that start with the issuing of a warning, seizure of the entire sum, or imposition of an administrative fine. Where criminality is suspected, the matter is referred to the police. The data supplied for 2024 records the use of these sanctions in 9 instances, with an average fine imposed of EUR 800, with a single referral to the police. The data is not sufficient to provide a basis for a detailed assessment of effectiveness of the impact of sanctions, however as already noted, the inconsistency

between detection by FARS, and the police clearly demonstrates that the controls are not effective in identifying cash and BNIs in transit. Equally, the sanctions are not dissuasive. If the average fine is compared to the average amount of undisclosed cash EUR 24 486 the fine represents a 3.26% penalty.

Chapter 9. Terrorist Financing Investigations and Prosecutions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.9 The Recommendations relevant for the assessment of effectiveness under this chapter are R. 5, 30, 31 and 39 and elements of R. 1, 2, 15, 32, 37 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Slovenia has a sound legal and institutional framework for combating TF. A variety of sources is used to identify TF activity. However, proactive identification of potential TF activity is rare: Slovenia does not employ OSINT or tactical/strategic analysis to identify potential TF activity and analyse emerging TF trends and techniques.

b) Since 2020, the competent authorities have initiated 16 pre- investigations on TF, all of which have ultimately been dismissed. The competent authorities (FIU, Police and SOVA) demonstrated a good level of operational cooperation and prioritisation in these cases. There is also an overall good theoretical understanding of the scope of TF offence and different roles that can be played by terrorist financers.

c) Slovenia has not prosecuted any TF cases and has not had any TF convictions. Therefore, it is not possible to comprehensively assess to what extent is TF activity prosecuted, and offenders convicted, nor the effectiveness of sanctions. Nevertheless, there are measures in place indicating that Slovenia is prepared to deal with TF prosecutions and judicial proceedings. These include specialised SPO prosecutors with regular trainings, review of key prosecutorial decisions by the head of the SPO. Judges also receive regular training on terrorism-related matters, including TF.

d) Slovenia has developed a National Strategy on Prevention of Violent Extremism and Terrorism. However, TF prevention gets little attention in it, and it was not informed by intelligence obtained through TF investigations. Overall, the importance of TF investigations appears to be under-appreciated by Slovenia.

e) Slovenia, in line with its risk and context, has also not applied any alternative measures when securing a TF conviction was not practicable.

Key Recommended Actions (KRA)

a) Slovenia should ensure more proactive approach to identification and investigation of TF, by employing OSINT and strategic/tactical analysis and to regularly monitor the changing TF trends and risk profile on a strategic level.

Other Recommended Actions

a) Slovenia should ensure that investigators and prosecutors are regularly and properly trained on evolving TF threats and methods.

b) Slovenia should incorporate the results of its TF cases into the formulation of its CT strategies.

Overall Conclusions on IO.9

Slovenia has a sound legal and institutional framework for combating TF. Authorities use variety of sources to identify TF activity, however, proactive identification of potential TF activity is rare. Slovenia does not employ OSINT or tactical/strategic analysis to identify potential TF activity and analyse emerging TF trends and techniques. While the AT considers that there should be more proactivity in their approach, these shortcomings call for major rather than fundamental improvements in Slovenia, given the risk and context of the country.

Since 2020, the competent authorities have initiated 16 pre- investigations on TF, all of which have ultimately been dismissed. Consequently, Slovenia has not prosecuted any TF cases and has not had any TF convictions. Operational cooperation and prioritisation between competent authorities (FIU, Police, and SOVA) has been demonstrated. Slovenia has also not applied any alternative measures when securing a TF conviction was not practicable which is in line with country's risk profile.

Although Slovenia has not prosecuted or convicted any TF cases, existing measures — including specialised SPO prosecutors with regular training, review of key prosecutorial decisions, and judicial training on terrorism-related matters — ensure that the authorities are prepared to handle TF cases if they arise.

TF prevention is given little attention in national counter-terrorism strategies, which are not informed by intelligence obtained in TF investigations.

Overall, the AT considers that, despite identified weaknesses Slovenia's system proved ability to identify and prioritise TF and measures which ensure adequate prosecution of such cases. On this basis the AT concludes that Slovenia achieved IO.9 to some extent. Important deficiencies have been identified; however, they are given appropriate weight considering Slovenia's risk and context, leading the AT to the conclusion that major improvements are needed

Slovenia is rated as having a moderate level of effectiveness for IO.9.

9.1. TF activity identified and investigated

640. Slovenia has a sound legal and institutional framework for combating TF, with security and law enforcement authorities having a good understanding of the country's TF threats and TF techniques.

9.1.1 Identification and investigation of TF activity

641. The competent authorities for identification of TF in Slovenia are the Slovenian Intelligence and Security Agency (SOVA) and police being the primary law enforcement agency responsible for conducting

TF pre-investigations. Once the cases are identified, prosecutors shall make a motion to the investigative judge to open a criminal investigation.

642. Slovenia uses variety of sources to identify TF activity including: FIU's financial intelligence (stemming from STRs submitted by OEs), SOVA's domestic intelligence, information and requests received from foreign counterparts and parallel financial investigations. Other sources – such as OSINT or information gathered through risk-based supervision of NPOs or tactical/strategic analysis of transactions involving cross-border payments to/from high-risk TF-related jurisdictions – have not been used in identification of TF cases.

643. Slovenian police take part in international and regional initiatives for combating TF, such as Europol Terrorist Finance Tracking Programme and EU Counter Terrorist Financing Investigators Network. Such initiatives contribute to its ability to detect and combat TF more effectively.

644. The competent authorities (FIU, SOVA, the police and the SPO) have dedicated staff in place for counterterrorism or TF purposes. Most of them have received some specialised training on TF; however, the authorities are missing additional training on the evolving TF threats and trends, especially in relation to emerging global threats. In addition, the police and SPO noted that understaffing and departures of experienced staff members in the police in general (see more under IO.7) can also negatively impact the investigation of TF.

645. Since 2024 Police and prosecutors face legal impediments to obtain timely financial information and apply covert investigative measures which can have negative impact on the identification of TF offences (see more under IO.7).

646. There are no formal policies or procedures to govern the prioritisation of TF cases. Nevertheless, the competent authorities (FIU, Police and SOVA) demonstrated a good level of operational cooperation and prioritisation of TF cases in practice. For example, TF-related STRs are in practice prioritised by the FIU.

647. Case Box 9.1. demonstrates a case where an OE, the FIU, SOVA and the police cooperated effectively and prioritised a potential TF case.

Case Box 9.1. TF identification and prioritisation

In February 2024, a Bank in Slovenia identified noticeable signs of radicalisation of its customer, which triggered further due diligence of that customer. Consequently, the bank identified some suspicious outgoing transactions of that customer to various foreign NPOs. The next day after performing the due diligence, the bank informally notified the FIU it would submit a TF-related STR, and the bank proceeded to submit the STR without delay.

Upon receipt of the STR, FIU prioritised it and initiated operational analysis, requesting further financial intelligence from OEs, 10 foreign FIUs, as well as promptly informed SOVA and the police. The FIU gathered a comprehensive financial intelligence file, encompassing over 200 suspicious outgoing transactions to foreign NPOs in 8 countries in an amount exceeding EUR 8 000.

The FIU, SOVA and the police demonstrated a good level of cooperation. All authorities met onsite were familiar with the facts of the case and confirmed ongoing cooperation.

The case is still ongoing. FIU continues to monitor financial transactions of the bank's customer; SOVA continues monitoring the activities of the person exhibiting radicalisation signs. The police had opened a pre investigation, which was still ongoing at the time of the onsite visit.

Source: Onsite interviews with FIU, SOVA and the police.

648. The competent authorities have demonstrated overall good level of understanding of inherent TF threats, theoretical understanding of the scope of TF offence and different roles that can be played by terrorist financers. Nevertheless, the absence of caselaw and therefore hands-on experience with judicial investigation and prosecution of TF may raise concerns if there is comprehensive practical understanding of elements of TF offences. For example, one key authority was not sure if sending weapons to a known terrorist organisation would constitute a TF offence. This raises concern regarding the level of understanding of the scope of TF offences among relevant authorities.

649. Since 2020, the Police has initiated 16 pre-investigations on TF (see breakdown by year in Table 9.1.), all based on FIU's disseminations. 6 disseminations were based on information supplied by foreign FIUs. 3 disseminations were based on the information contained in the STRs submitted to the FIU by OEs. 7 of those disseminations had originated from domestic intelligence submitted to the FIU by either SOVA or police for the FIU to execute financial inquiries. After carrying out financial inquiries acting on the information supplied by SOVA or the police, the FIU compiled financial intelligence and disseminated it to the police for pre- investigations on TF.

Table 9.1. Number of TF pre-investigations per year

Source	2020	2021	2022	2023	2024	TOTAL
FIU dissemination	7	1	2	2	4	16

Source: Police

650. The police, as the responsible investigative authority, undertakes pre-investigation of TF. Initial criminal reports are submitted to the prosecutor (SPO), which is responsible for assessing the case, agreeing and preparing applications to the court for investigative orders. 13 of the TF pre investigations were closed by the police because there were no reasonable grounds to suspect the commission of a TF offence. Most of these pre-trial investigations involved suspicious transactions executed by Slovenia-registered legal persons with BOs from high-risk jurisdictions. Police employed appropriate measures in order to determine potential TF suspicion and found no grounds for suspicion of TF.

651. In 3 TF pre- investigations, the Police submitted reports to the SPO. All 3 cases were dismissed due to the lack of proof regarding relevant elements of the crime. However, the AT was not assured about the reasonableness of dismissing of one of those cases.

Case Box 9.2. Dismissing TF investigation by the police and the SPO

Based on information received from a foreign FIU, Slovenian FIU disseminated a case to the police in relation to suspicious transactions carried out from 5 June 2020 to 23 November 2022 in the amount of EUR 61 976.19, involving multiple persons and jurisdictions.

The information noted that, among other transactions, a Slovenian citizen (Person A) and a citizen of Bosnia and Herzegovina (Person B) had carried out several suspicious monetary transactions via fictitious accounts in one foreign FI and one Slovenia-registered FI to a citizen of a foreign country (Person C), who was allegedly a member of a designated terrorist organisation The alleged purpose of these transactions was to recruit individuals from the Balkan region into terrorist groups.

Persons A and B received suspicious funds via foreign FI into their accounts with the Slovenia-registered

FI, which they subsequently partially withdrew in cash, partially converted into crypto assets, and partially transferred to accounts of suspicious user profiles in the foreign FI. The total amounts transferred by Persons A and B were in an amount less than EUR 1 000.

SPO was notified of the case. SPO instructed that data be obtained from foreign security authorities to confirm whether Person C was indeed a member of a terrorist group or engaged in terrorist activities. Through the International Police Cooperation Sector, a request was sent to the authorities of a foreign country for operational information regarding all involved persons, including all operational data confirming the Person C's membership in terrorist organisation and any record of criminal activity No responses had yet been received.

Police and SPO had not conducted interviews with Persons A and B to prevent compromising the investigative operations of foreign security authorities. SPO dismissed the case on 5 September 2023, for, among other, citing the following reasons: (1) Person C's terrorist activities had not been verified; (2) Most transactions by Persons A and B were sent to accounts of unknown users, and only a few accounts were allegedly linked to Person C, meaning it was not established that Person C actually received the funds; (3) There is no evidence that Persons A and B knew the funds would be used for terrorist acts or directed to terrorist organisations; (4) the amounts involved were minor, intended as family aid or cryptocurrency purchases, thus lacking the essential *mens rea* element for TF.

Source: Onsite interviews and post onsite information provided by the police and SPO.

652. Looking solely at this pre-investigation (Case Box 9.2.), the dismissal of the TF investigation did not seem fully substantiated to the AT, as there were more avenues to pursue in order to comprehensively address the potential TF. The AT has concerns about the reasonableness of not conducting the interviews with the persons involved and citing low monetary value of potential TF transactions as a justification for dismissing the case. Overall, the importance of thorough investigation of any TF suspicion did not appear to be fully reflected in the SPO' approach.

9.1.2 Investigations identifying the specific role of terrorist financier

653. The competent authorities are systematically conducting parallel financial investigations into potential TF. 7 of the 16 TF pre-investigations had originated from domestic intelligence submitted to the FIU to execute financial inquiries. Even though no formalised procedures exist in that regard, terrorism-related cases are always also referred to the FIU for parallel financial investigations, which can contribute to identifying the roles of terrorist financiers.

9.2. Prosecuting and convicting different types of TF

654. Slovenia has not prosecuted any TF cases. Therefore, it is not possible to assess the extent to which TF activities (including different types of TF cases) are prosecuted, and offenders convicted. However, the AT took a broader approach to assess the authorities' capacity in the event of a TF case. The SPO is competent authority to prosecute TF offences. Within this unit, there are specialised prosecutors for terrorism and TF matters who receive regular training. While there is no training solely dedicated to TF offences, authorities provided evidence of various trainings attended by prosecutors and judges on terrorism-related matters, illicit use of crypto assets, including for TF purposes.

655. In addition, no formal or informal guidelines for SPO prosecutors exist in Slovenia exclusively for prosecuting TF offences. Nevertheless, measures are in place to ensure that TF cases receive additional

scrutiny, if they were to occur. For example, decisions on the dismissal of a TF case or the submission of an indictment, must be submitted to the head of the SPO before they are finalised. The head of the SPO should review the case and may take over the case if they establish that there are deficiencies in handling the case by the prosecutor. The AT considers that these practices provide additional oversight, particularly over the dismissals of TF cases.

656. There are no specialised judges for TF cases in Slovenia. Nevertheless, judges undergo regular training on terrorism-related matters, which also covers issues related to TF offences.

657. Overall, the AT concludes that, due to the absence of practical cases, it is not possible to comprehensively assess Slovenia's prosecution and conviction of TF offences. Nevertheless, the measures described above indicate that the authorities have the capacity to handle TF cases.

9.3. Effectiveness, proportionality and dissuasiveness of sanctions

658. Slovenia has not had any TF convictions. There are no specialised judges for TF cases in Slovenia and there are no sentencing guidelines for TF or similar offences. Very few existing terrorism convictions (most of which were outside the reporting period) do not provide for meaningful examples to conclude whether sanctions for TF would be effective, proportionate and dissuasive. Therefore, it is not possible to assess to what extent the sanctions or measures applied against natural and legal persons convicted of TF offences are effective, proportionate and dissuasive.

9.4. National counter-terrorism strategies and activities

9.4.1 Formulating national counter-terrorism strategies and activities

659. Slovenia has adopted the National Strategy on Prevention of Violent Extremism and Terrorism. On TF issues, the strategy is brief:

660. "The legislation and system governing the prevention of ML are consistent with international legal acts and standards. The OEs comply consistently with their duties to report suspected TF detected on the basis of a list of indicators and adopt all the necessary measures in accordance with the AML/CFT Law. Considering the fact that the fight against terrorism, violent extremism, and TF is a global issue, international cooperation is important in the prevention of ML/TF. The Republic of Slovenia will continue to carry out, upgrade, and strengthen activities to prevent ML/TF."

661. The AT concludes that the national policies in relation to TF prevention are formulated broadly and given little attention. Information and intelligence obtained in TF investigations, as well as information on TF risk assessment, TF trends and techniques was not used in the formulation of National Strategy on Prevention of Violent Extremism and Terrorism.

9.4.2 Sharing and using information and intelligence to support national counter-terrorism purposes and activities

662. Information and intelligence obtained in TF investigations was not used to support national counter-terrorism purposes and activities. One authority claimed that TF investigations yielded no information or intelligence that could be used to support national counterterrorism strategies and activities. Nevertheless, the AT was not assured that such information and intelligence would be used, even if it was available. The topic of TF investigations is largely overlooked in national counter-terrorism strategies.

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

663. In Slovenia, various alternative measures can be applied when securing TF conviction is not practicable, including monitoring of high-risk individuals, pursuing other terrorism-related offences or proposing a designation of a person under TFS regimes (see more under IO.10).

664. However, in line with Slovenia's risk and context, the competent authorities of Slovenia have not thus far applied any other measures if securing a TF conviction was not practicable.

Chapter 10. Terrorist Financing Preventive Measures and Financial Sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.10. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 1, 4, 6 and 8 and elements of R.14, 15, 16, 26, 30, 31, 32, 35, 37, 38 and 40.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) TF TFS adopted pursuant to UNSC Resolutions (UNSCRs) 1267/1989, 1988 and 1373 are applicable in Slovenia without delay. Slovenia has a procedure and a mechanism for identifying targets for designation, however, no designations were made or proposed by Slovenia under the UNSCRs, which is in line with its TF risk profile.

b) Implementation of TF TFS without delay can be hampered in practice by the lack of a proactive mechanism to communicate designations to OEs and the general public, which is a major shortcoming. FIs and VASPs generally employ commercial screening tools hence they are less exposed to it. OEs were provided with Guidance for implementation of TFS, which also have not been properly communicated to the OEs, except for FIs supervised by the BoS. This issue is partly attributed to the lack of adequate resources and staffing in the MFEA.

c) Governance framework of Slovenia for the implementation of TFS has a number of weaknesses evidenced by the lack of: (i) clear channels of communication and the central authority for the receipt of reports on implementation of TFS; (ii) clarity on reporting obligations and format for reporting; (iii) statistics on TFS reporting; and (iv) ability to demonstrate steps taken on reported freezing or rejected transactions.

d) Slovenia carried out some NPOs TF risk assessments in the reporting period. Those did not lead to proper identification of the subset of NPOs that fall under the FATF definition and proper identification of the TF risks posed to them. Slovenia does not apply focused, proportionate and risk-based mitigation measures to NPOs. The governance framework for oversight and monitoring of NPOs is decentralised, fragmented and lacking coordination.

e) Material FIs and VASPs have a solid understanding of their TF-related TFS obligations and established effective policies, procedures and controls to ensure compliance with them. DNFBPs generally demonstrate a low level of understanding of and compliance with obligations in relation to the implementation of TF-related TFS.

f) Supervisors for FIs and VASPs are generally monitoring and ensuring compliance by FIs, VASPs within the framework of the full-scope inspections. There are major deficiencies in monitoring and ensuring compliance by DNFBPs in relation to TF-related TFS obligations.

Key Recommended Actions (KRA)

a) Slovenia should establish an efficient method to communicate the UN TFS designations on TF to OEs and the general public.

b) Slovenia should (i) establish a clear reporting channel and standard form for OEs to report to the MFEA on frozen assets and attempted transactions, in line with relevant UNSCRs; (ii) designate a specific MFEA contact point to receive these reports; (iii) ensure the designated recipient has sufficient capacity (including staffing) to act on reports; and (iv) ensure all OEs are informed of the reporting form and channels.

c) Slovenia should: (i) identify the subset of organisations falling under the FATF definition; (ii) conduct an in–depth and comprehensive risk assessment of those NPOs to identify the nature of TF risk posed to them; (iii) develop focused, proportionate and risk-based measures to address TF risks and the oversight with clearly defined and coordinated responsibilities.

Other Recommended Actions

a) Slovenia should ensure that the DNFBPs establish effective policies, procedures and controls to ensure compliance with UN TFS.

b) Slovenia should improve monitoring framework and ensuring compliance by DNFBPs with the UN TF-related TFS obligations, including through a regular outreach.

Overall Conclusions on IO.10

TF TFS adopted pursuant to UNSCRs are applicable in Slovenia without delay. Authorities do not conduct active communication of designations to OEs, which is an important issue, but this does not affect the most material OE sectors. Governance framework of Slovenia for the implementation of TFS has a number of weaknesses affecting the effectiveness of the framework.

While the FIs and VASPs which represent the material sector of OEs overall have adequate understanding of their obligations, and mechanisms to ensure compliance with UN TFS on TF, including effective policies, procedures and controls, the situation is different with the DNFBP sector, which has a low level of understanding of and compliance with obligations in relation to the implementation of TF-related TFS.

In general, in contrast to the one for the DNFBPs, the supervisory framework for FIs and VASPs functions adequately.

While Slovenia had conducted the assessment on the risk of TF abuse of NPOs in multiple occasions, those assessments did not prove to be comprehensive and did not contribute to establishment of focused, proportionate and risk-based measures, including the oversight. The governance framework for oversight and monitoring of NPOs is decentralised and fragmented with the coordination being an issue.

Slovenia is rated as having a moderate level of effectiveness for IO.10.

10.1. Implementation of TF-related targeted financial sanctions without delay

665. Since 2022, Slovenia's legal framework enables the immediate implementation of targeted financial sanctions (TFS) for TF, pursuant to United Nations Security Council Resolutions (UNSCRs) 1267/1989 and 1988. This compensates for delays in transposing UN designations at EU level. Slovenia also implements TF-related TFS through the directly applicable EU regulations and its Act on Restrictive Measures (RMA).

666. Slovenia has not proposed any designations pursuant to UNSCR 1267/1989 and 1988. It has not received any requests from other countries. Slovenia has also not individually initiated designation pursuant to UNSCR 1373 at the domestic level and at the EU level, which is consistent with Slovenia's TF risk level, which is low.

667. The SCG – chaired by the MFEA – has adopted a procedure and mechanism for identifying targets for designation. Under this procedure, SCG's Sanctions Lists Sub-Group considers duly reasoned proposals from members of the SCG or from foreign counterparts. The authorities demonstrated that the relevant procedures would be implemented in practice when needed.

668. In Slovenia, the MFEA is responsible for policymaking in the field of TFS and acts as the country-level co-ordinating body for implementation of TFS. There are two employees dedicated to implementation of TFS (not only UNSCRs, but also all autonomous EU sanctions regimes, the scope of which has significantly amplified during the reporting period), in addition to other responsibilities not related to the implementation of TFS. The MFEA, as well as other competent authorities and OEs noted understaffing and lack of resources in the MFEA as an impediment to effective functioning of the framework for implementation of TFS.

669. Slovenia has not introduced a mechanism for actively communicating designations to OEs and the general public in a timely manner. The only forms of communication of designations to OEs and the general public by the competent authorities is the availability of a link to the website of the UNSC, that is provided on the website of MFEA and in the TFS Implementation Guidelines. No other actions are taken by the competent authorities to make sure that OEs are aware of designations and to implement sanctions without delay. The absence of proactive communication was partly attributed to understaffing of the MFEA.

670. The competent authorities agreed that under such circumstances, failure to implement TF-related TFS without delay is possible, but improbable, since the FIs and VASPs employ commercial screening tools for compliance with TFS, which contain up to date information on designated persons and entities, and monitor transactions automatically, including over the non-working hours and weekends. Most of DNFBPs advised to check the customers against the TFS sanctions lists online. Also, DNFBPs generally do not work outside working hours. Nevertheless, even though the most material sectors are less exposed, the lack of proactive communication mechanism of designations to OEs in a timely manner is a major shortcoming. Even if FIs would be able to implement TF-related TFS without delay (e.g. ensure freezing of funds), there is a risk that other types of assets would not be identified efficiently and frozen without delay. MFEA – as the coordinating authority – could coordinate the identification of other assets of designated persons (and those acting on their behalf); however, the understaffing in the MFEA would also hamper its ability to do that effectively.

671. Slovenian authorities – Permanent Coordination Group on Restrictive Measures (also known as Sanctions Coordination Group or SCG) have developed "Guidelines for the effective implementation of restrictive measures" (TFS Implementation Guidelines) to provide guidance for the operational implementation of restrictive measures (i.e. sanctions, including TFS) in accordance with UN, EU and Slovenian regulations. TFS Implementation Guidelines were updated in February 2025. However, the TFS Implementation Guidelines have not been properly communicated to the OEs, except for FIs supervised by

the BoS. This is due to a weak coordination among the competent authorities and also understaffing of the MFEA.

10.2. Identification and deprivation of terrorist funds or other assets

672. Slovenia has not identified any designated individual or entity under UNSCR-related TFS for TF, nor have funds been frozen under this framework, which is consistent with the low TF risk profile.

673. However, Slovenia demonstrated its governance framework for the implementation of TFS (and its ability to identify assets of terrorists, terrorist organisations and terrorist financiers and ability to prevent such persons and entities from raising, moving and using assets) to have a number of weaknesses. This, among others, is evidenced by the lack of: (i) clear channels of communication and the central authority for the receipt of reports on implementation of TFS; (ii) clarity on reporting obligations for the OEs and format for reporting; (iii) ability to maintain statistics and develop examples of reports received in regard to a (false positive) match with the UN TFS; (iv) ability to describe the undertaken steps where case of reporting and asset freezing or transaction rejection would occur. Therefore, in case funds subject to asset-freeze were identified and frozen by FI without delay, the AT was not assured about the effectiveness of follow-up steps taken by the competent authorities after receiving a report about the respective asset-freeze, e.g. if Slovenia would be able to identify and freeze, without delay, other types of assets of designated persons and entities and those acting on their behalf or at their direction.

674. The competent authorities and OEs provided diverse information on the manner of reporting, and channels for communication. Some have mentioned the MFEA, some mentioning their supervisors and some – the OMLP. The authorities advised and the OEs confirmed that there is no developed template for reporting matches with designated persons and frozen assets or rejected transactions. The OEs would either use the STR form or draft a free-format e-mail. All those authorities have confirmed receiving sporadically reports on matches with designated persons (under autonomous EU sanctions regimes). As a result, none of the mentioned authorities gathered comprehensive data on implementation of TFS in the country. The authorities could not also explain the systemic approach applied to dealing with the received reports, creating gaps in understanding of the scope of assets frozen, data accessibility, its analysis and, therefore, hampering the effectiveness of implementation of TFS.

675. Therefore, Slovenia was not able to demonstrate operational readiness to effectively identify terrorists (including designated persons) and prevent them from raising, moving and using funds or other assets.

10.3. Targeted application of focused and proportionate mitigation measures to at-risk non-profit organisations

676. In 2020, Slovenia conducted an analysis of NPOs' TF risks. However, the risk assessment did not lead to proper identification of the subset of NPOs that fall under the FATF definition of NPO. NPO Strategic Analysis concluded that there are 17 NPOs that potentially pose higher TF risk. The NRA 2021 does not reflect on the exact number of those. The ongoing analysis suggests that there are some foundations and some association with status of humanitarian organisations to potentially pose higher TF risk. Consequently, these studies do not support each other's findings and leave uncertainties on the nature of TF risks posed to NPOs. Authorities advised that they will need to further explore the subject.

677. Slovenia had also explored the risks related to abuse of NPOs for TF purposes within the scope of the NRA 2025. While the approach as also previously would not focus on the NPOs per the FATF definition, it gives and overall overview of the risk picture in the country. The analysis concludes that the threat of TF remains low in Slovenia, but it is potentially present, particularly through the abuse of NPOs. The NRA also

explores the observed risks related to servicing the NPOs as customers by FIs and DNFBPs. It concludes that there were no specific cases of NPO misuse for TF purposes detected by the OEs servicing those organisations. While this does not amount for a comprehensive analysis of the risks of misuse of NPOs for TF purposes in Slovenia, this analysis would suggest that overall, the probability of happening so is rather low.

678. While, in general, the findings of the NRA 2021 and 2025 were shared with the OEs, the findings of the NPO TF risk assessment from 2020 were not communicated to competent authorities, OEs or to the NPO sector. Slovenian authorities have not conducted sustained outreach on the TF risks within the NPO sector and the donor community. The NPOs advised that there has been no guidance from the competent authorities in relation to addressing TF risks in the NPO sector. The NPOs themselves were generally not familiar with the TF risks in the NPO sector.

679. Slovenia applies multiple mechanisms to promote accountability, integrity and public confidence in the administration and management of NPOs. This is done through multiple mechanisms, including the requirement for registration of the Non-Governmental Organisations (NGOs), regulatory framework for obtaining the status of an NPO, tax accountability, etc.

680. Slovenia advised also to implement a Strategy for the development of NGOs in the Republic of Slovenia 2018-2023 that includes a strategic goal of promoting transparency, integrity, and accountability of NGOs. But this strategy was not informed by the NPO risk assessment. Nevertheless, Slovenia maintains a dialogue with the non-profit sector, and exchange on best practices through various means and channels.

681. Majority of Slovenian NPOs operate domestically, supporting their specific target groups. A number of NPOs were operating in the field of implementation of specific government projects, being funded by e.g. Ministry of Education, Health etc. There were two NPOs which are part of international organisations that were specifically collecting funds to support the vulnerable persons in one the ongoing conflict zones. Those had suggested that collected funds were not distributed by them directly, but these would be centralised in the headquarter and further distributed from there.

682. The governance framework for oversight and monitoring of NPOs is decentralised and fragmented, involves multiple competent authorities (see also c.8.3), with a coordination being an issue. Slovenia does not have in place focused, proportionate and risk-based measures to conduct monitoring of NPOs. The only available detailed information is available on the oversight carried out through tax audits. TF indicators are not assessed within tax audits of NPOs.

Table 10.1 Number of tax inspections at non-profit organisations in the last 5 years (2020-2024)

Tax audits/inspections at non-profit organisations (NPOs)	2020	2021	2022	2023	2024
institute	20	16	37	14	13
public economic institute	8	111	112	19	11
institution	1	0	1	0	0
associations	43	93	76	36	13

683. These inspections detected certain breaches which were all related to pure tax declaration/payment issues. No issues related to breach of legislation that would indicate TF risks were identified.

10.4. FIs, VASPs and DNFBPs understanding of and compliance with obligations

10.4.1 FIs and VASPs

684. Most of the FIs and VASPs have established (in accordance with the requirements of the competent authorities) effective policies, procedures and controls to ensure compliance with UN TFS and timely detection of breaches of those measures. While certain deficiencies were observed in the smaller, non-material FIs, this was also confirmed by the findings of supervisory authorities.

685. The majority of FIs and VASPs, especially the most material ones, demonstrated a solid understanding of their TFS obligations and the requirement to freeze the assets of designated individuals or entities. They primarily use automated screening tools, which are kept up to date with the latest UNSCR listings. FIs and VASPs had procedures and sufficient resources to manage potential matches and discard false positives.

686. FIs and VASPs typically have advanced, real-time screening systems, ensuring TFS implementation upon customer onboarding and throughout the business relationship. Those checks are conducted on the customers, but also their BOs and transactions. Internal policies and controls enable timely identification and reporting of (false positive) matches.

687. None of the FIs/VASPs had a genuine TF-related TFS hit, which is in line with country's risk profile.

10.4.2 DNFBPs

688. DNFBPs generally demonstrate a low level of understanding of and compliance with obligations in relation to the implementation of TF-related TFS.

689. Most of the DNFBPs were familiar with the concepts of UNSCRs and sanctions screening obligations, except for casinos, the real estate entities, and DPMS. The DNFBPs were generally unaware of the existence of Sanctions Implementation Guidelines. In addition, the absence of a communication mechanism negatively impacted timely awareness of changes to UNSCRs and therefore their implementation without delay especially in the three mentioned sectors.

690. Checks conducted by the DNFBPs except for the ones that are part of an international groups (law firms, audit etc.) were basic. These checks were confined to verifying the name of the customer or the party directly involved in the transaction with the UN TFS as published online. The other parties, such as BOs, other directly or indirectly concerned entities and persons were not checked.

691. Many supervisors of DNFBP sectors agreed that the level of understanding of and compliance with obligations in relation to the implementation of TF-related TFS in DNFBP sector is limited.

10.5. Competent authorities monitoring and ensuring compliance with TF-related targeted financial sanctions

10.5.1 FIs and VASPs

692. BoS and ISA generally monitor the implementation of TF-related TFS within full scope on-site inspections; however, the authorities were not able to provide clear statistics on inspections carried out. BoS also performs certain outreach measures in the form of publishing information, issuing guidance and providing training. However, these activities are not targeted specifically to TF-related TFS. Employees of the BoS also have not received a separate training on TF-related TFS.

693. Inspections conducted by BoS indicate that most FIs and VASPs are generally compliant with TFS obligations. BoS has not detected any serious breaches in the banking sector. Within the carried-out examinations, BoS concluded that banks effectively screen their customers and transactions for TFS and identified only comparatively immaterial breaches (e.g. insufficiently detailed organizational procedures for implementation of TFS, lack of targeted trainings on TFS, inconsistencies regarding periodic checks). The follow-up inspection had confirmed that those breaches were rectified.

694. Within the exchanges office sector, BoS established that those performed the checks manually and frequently failed to maintain adequate records as required by their internal policies. Through subsequent follow-up procedures, BoS determined that these deficiencies had been effectively remedied.

695. BoS and ISA have not imposed any fines for infringement in relation to compliance with TF-related TFS.

Case Box 10.1. BoS inspection on TFS implementation in a bank

In line with the supervisory plan of BoS, in 2023 it conducted a targeted inspection focused on compliance of one bank with the TFS, including TF-related TFS. The particular bank was comparatively more exposed to sanctioned entities or persons to evade sanctions. Through sample testing, the BoS did not identify breaches, evasion or non-implementation of TF-related TFS. BoS found that bank complies with TFS binding in accordance with the RMA. Nevertheless, BoS recommended the bank to enhance and improve effectiveness of its sanctions policies, processes and controls, namely, including to implement IT support for timely sanctions screening of the customer database. The bank remediated all the shortcomings.

696. SMA and ISA advised to conduct a number of inspections to monitor the supervised OEs, but those were not related to the UN TFS framework. The FARS have not recorded any activities to monitor and ensure compliance with TF-TFS by the OEs under its supervision. Employees of ISA, SMA and FARS also have not received a separate training on TF-related TFS.

697. Competent authorities have informed FIs and VASPs about the Sanctions Implementation Guidelines; however, no other targeted guidance or outreach in relation to the implementation of TF-related TFS has been provided to FIs and VASPs.

10.5.2 DNFBPs

698. Competent authorities do not systematically conduct monitoring and ensuring compliance with TF-related TFS. In the period under review, no such inspections have been carried out.

699. The perceived level of risk of DNFBPs being involved in breach, evasion or non-implementation of TFS, differs significantly among the supervisors of DNFBP sectors, ranging from low to medium-high. This discrepancy demonstrates that the risk is not fully understood and appreciated in the DNFBP sector.

700. Competent authorities had not informed DNFBPs about the Sanctions Implementation Guidelines, which are available online. No other targeted guidance or outreach in relation to the implementation of TF-related TFS has been provided to DNFBPs.

Chapter 11. Proliferation Financing Financial Sanctions

The relevant Immediate Outcomes considered and assessed in this chapter is IO.11. The Recommendations relevant for the assessment of effectiveness under this chapter are R. 7 and elements of R.1, 2 and 15.

Key Findings, Recommended Actions, Conclusion and Rating

Key Findings

a) Slovenia has established a SCG to ensure uniform implementation of UN TFS on PF that encompasses a broad range of competent authorities. Slovenia has also demonstrated well-developed operational cooperation practices among the SOVA, Police and the OMLP. While the Foreign Policy Strategy would generally reflect on Slovenia's commitment on counter-proliferation matters, it does not have a dedicated CPF policy.

b) Slovenia conducted its first PF risk assessment within NRA 2025. Its comprehensiveness is limited. The PF risk is assessed as low and risk of breach, non-implementation or evasion of PF-related TFS in some OEs (banks and DNFBPs), was also assessed to be low, except for the VASPs where the level of PF threat was assessed to be medium-high. Slovenia did not demonstrate specific measures to mitigate the PF risks.

c) PF TFS adopted pursuant to UNSCRs 1718 and the subsequent resolutions are applicable in Slovenia without delay. The mechanism and shortcomings for implementation of PF related TFS are similar to TF related TFS for TF (see IO.10).

d) Governance framework of Slovenia for the implementation of TFS has a number of weaknesses, which are identical for TF and PF sanctions regimes (see IO.10).

e) FIs and VASPs have a good general level of understanding of their PF-related TFS obligations. However, they are mostly unaware of typologies related to the evasion of PF-related TFS. DNFBPs generally demonstrate a low level of understanding of and compliance with obligations in relation to the implementation of PF-related TFS. There are significant deficiencies in monitoring and ensuring compliance by DNFBPs in relation to PF-related TFS obligations.

Key Recommended Actions (KRA)

a) Slovenia should establish an efficient method to communicate the UN TFS designations on PF to OEs and general public.

b) Slovenia should develop a methodology and utilise a variety of sources to identify, assess, and understand the risk of PF breaches, non-implementation or evasion present in the country and take measures to mitigate those risks.

c) Slovenia should (i) establish a clear reporting channel and standard form for OEs to report to the MFEA on frozen assets and attempted transactions, in line with relevant UNSCRs; (ii) designate a specific MFEA contact point to receive these reports; (iii) ensure the designated recipient has sufficient capacity (including staffing) to act on reports; and (iv) ensure all OEs are informed of the reporting form and channels.

Other Recommended Actions

a) Slovenia should ensure that the DNFBPs establish effective policies, procedures and controls to ensure compliance with UN TFS measures.

b) Slovenia should improve monitoring framework and ensuring compliance by DNFBPs with the UN PF-related TFS obligations, including through a regular outreach. All OEs should be made aware of global typologies on evasion of UN TFS on PF.

Overall Conclusions on IO.11

Slovenia has established the SCG in order to ensure uniform implementation of sanctions, chaired by a representative of the MFEA and encompassing a broad range of competent authorities. In addition, SOVA, Police and OMLP have demonstrated to have well-developed operational cooperation practices.

Slovenia conducted its first PF risk assessment within NRA 2025, concluding that the country's national PF risk is low. Its comprehensiveness is limited. Authorities had uneven understanding of the PF risks in Slovenia and globally.

PF TFS adopted pursuant to UNSCRs are applicable in Slovenia without delay. Authorities do not conduct active communication of designations to OEs, which is an important issue, but this does not affect the most material OE sectors. Governance framework of Slovenia for the implementation of TFS has a number of weaknesses affecting the effectiveness of the framework.

No assets have been frozen in Slovenia pursuant to PF-related TFS. However, the lack of clear lines of communication on implementation of TFS leads to poor quality of statistics and data, e.g. on transactions rejected.

FIs and VASPs have a good general level of understanding of their PF-related TFS obligations. They often utilise commercial screening tools and conduct regular checks. However, they are mostly unaware of typologies related to the evasion of PF-related TFS. Most of the DNFBPs demonstrated a low level of understanding of and compliance with obligations in relation to the implementation of PF-related TFS.

Competent authorities monitor and ensure compliance by FIs and VASPs with their obligations regarding PF-related TFS within their full scope on-site inspections and some off-site monitoring activities, which are not PF-targeted. However, there are significant deficiencies in monitoring and ensuring compliance by DNFBPs in relation to PF-related TFS obligations.

Slovenia is rated as having a moderate level of effectiveness for IO.11.

701. At the end of the on-site visit (10 October 2025), relevant UNSCRs in force relating to PF were Resolution 1718 pertaining to the Democratic People's Republic of Korea (DPRK) and subsequent Resolutions 1874, 2087, 2094, 2270, 2321 and 2356. At the EU level, UNSCR 1718 (2006) on DPRK and its successor resolutions are implemented through Council Decision 2016/849/CFSP and EU Regulation 2017/1509, the latter being directly applicable in Slovenia.

702. Slovenia does not have a direct exposure to the DPRK sanctions regime. There is no embassy in the country, no trade ties, no citizens of North Korea living in Slovenia and vice-versa. Based on the data analysis from 2020–2025 there were no transaction to or from North Korea conducted within the banking sector. Slovenia is not a financial centre and not a company formation centre.

11.1. Competent authorities co-operation and co-ordination to combat PF financing

11.1.1 Co-operation and co-ordination to develop and implement policy

703. Slovenia has established a Sanctions Coordination Group (SCG) to ensure uniform implementation of sanctions, chaired by a representative of the MFEA and encompassing a broad range of competent authorities – including Ministry of Finance, Ministry of Economy, Ministry of the Interior, Ministry of Defence, Ministry of Justice, BoS, SOVA, FIU and others. Members are required to be at the level of State Secretaries or similar high-level officials to ensure high-level decisions to be taken.

704. For technical issues relating to implementation of TFS, the SCG established a sub-group on financial sanctions, on sanctions lists (see more in Chapter 4.3.1.), and on criminal law issues relating to sanctions. Members of the Subgroup on financial restrictive measures have not encountered any cases of proliferation or PF, therefore, the Sub-group on financial sanctions has not held any discussions on implementation of PF TFS. This is overall in line with the context of Slovenia considering absence of known trade and financial ties with North Korea.

705. The MFEA had issued the Foreign Policy Strategy of the Republic of Slovenia in December 2024, which reinforces the commitment of the country to continue advocating for non-proliferation of weapons of mass destruction. Slovenia has not developed and implemented any CPF - specific policies.

11.1.2 Co-operation and, where appropriate, co-ordination for operational purposes

706. While the primary co-ordination framework established in Slovenia for PF matters is the SCG, the Ministry of Economy, Tourism and Sport (METS) is ensuring the co-operation and co-ordination of issues related to counter-proliferation matters being the ministry in charge of licensing of export of controlled and dual-use goods. It has its own standing group to support its decision-making process, in which the MFEA, Police and some other authorities are also represented. Where appropriate, through the shared members of the two standing groups, the METS may seek input from SCG members with expertise relevant to the specific sector concerned by the proposed export. These procedures demonstrate to some extent, the coordinated approach adopted by the Slovenian authorities in addressing CPF matters.

707. In addition, SOVA, Police and OMLP have demonstrated to have well-developed operational cooperation practices. These authorities exchange operational and intelligence information (including through licensing of cross-border movement of goods). While within the evaluated period Slovenia did not report to have cases engaging North Korea, the presented case example and co-ordinated operational measures taken would suggest that Slovenia has adequate operational mechanisms in place to respond to the threat of unauthorised movement of dual-use goods.

11.2. Understanding and mitigating the risk of breach, non-implementation or evasion of PF-related targeted financial sanctions

708. Slovenia conducted its first PF risk assessment within NRA 2025. The NRA concluded on the overall national level the PF risk and risk of breach, non-implementation or evasion of PF-related TFS in some OEs. Authorities and the OEs demonstrated uneven understanding of those risks, including in a global scale. This

demonstrated that the comprehensiveness of the conducted PF risk assessment is limited which was also acknowledged by Slovenia.

709. NRA 2025 concludes that at the national level the PF risk is low. The AT does not challenge the conclusion on the level of the risk bearing in mind the context of the country, per se. Nevertheless, this conclusion was not supported by demonstration of specific methodology and information sources used to identify, assess and understand the PF risks at the national level.

710. In addition, Slovenia had also conducted analysis of some risks, threats and vulnerabilities for evasion of PF sanctions within specific sectors, such as banking sector, VASPs and DNFBPs.

711. While the base for analysis, depth and the scope are uneven, the NRA 2025 concludes that: (i) within the banking sector the IT tools used are adequate to detect transactions with designated persons or entities and freeze the assets in a timely manner; (ii) within the VASP sector the anonymity of ownership of VAs, the irreversibility of and the international dimension of transactions brought the sector to the level of medium-high PF threat; (iii) within the DNFBP sector due to absence in the customer base of designated persons or entities, transactions with designated persons or entities, reported matches and frozen assets, the inherent risks in terms of proliferation financing are low, and for some sectors are insignificant. Nevertheless, this analysis is also based on a limited data.

712. Slovenia did not demonstrate specific measures designed for mitigation of risks of breach, non-implementation or evasion of PF. While no practical cases were detected, identifying potential evasion of PF related TFS may also be affected by certain shortcomings in identifying beneficial owners (see IO.5).

11.3. Implementation of PF-related targeted financial sanctions without delay

713. Since 2022, Slovenia's legal framework prescribes direct and immediate applicability of PF-related UN TFS in the country. Slovenia is relying on its domestic and also European legislation to implement obligations relating to PF related TFS[25].

714. Considering that Slovenia's legal framework governing the implementation of TFS applies equally to TF and PF related UN TFS, the institutional framework and the powers are identical to what is described under IO.10. In Slovenia, the MFEA is responsible for policy-making in the field of TFS and acts as the central authority for the operational matters related to the implementation of PF-related TFS. Its understaffing and lack of resources is an impediment to effective functioning of the framework for implementation of TFS in Slovenia.

715. Similar to the framework for implementation of the TF-related sanctions, Slovenia has not introduced a mechanism for actively communicating designations to OEs in a timely manner, the only form of communication being the availability of a link to the website of the UNSC, that is provided on the website of MFEA. While overall considered to be an important shortcoming, this, does not affect the most material OE sectors.

11.4. Identification of assets and funds held by designated persons/entities/those acting on their behalf and prohibitions

11.4.1 Identifying funds or assets held by designated persons/entities/persons acting on their behalf or at their direction

25. All UNSCRs that impose targeted financial sanctions associated with financing the proliferation of weapons of mass destruction are transposed into European law and apply directly in Slovenia.

716. Slovenia has not identified any designated individual or entity under UNSCR-related TFS for PF, nor have funds been frozen under this framework, which is consistent with the Slovenia's context. However, Slovenian authorities were not able to provide any statistics on reports from OEs on (false positive) matches with PF TFS lists or transactions rejected pursuant to PF TFS which could have evidenced the ability of OEs to potentially detect funds of designated persons.

717. Similarly to TF-related sanctions implementation, Slovenia's governance framework for the implementation of PF-related TFS has a number of shortcomings, including lack of clear channels of communication and the central authority for the receipt of reports on identified assets, clarity on reporting obligations for the OEs and format for reporting; ability to maintain statistics and develop examples of reports received in regard to a (false positive) match with the UN TFS; ability to describe the undertaken steps where case of reporting and asset freezing would occur. These shortcomings can, to some extent, be attributed to the understaffing of the MFEA.

11.4.2 Prohibiting financial transactions related to proliferation

718. In Slovenia any natural and legal person is prohibited from making funds, other assets or economic resources available to persons designated under UNSCRs. This prohibition is implemented through the EU legislative framework and the domestic one. Under the domestic framework the breach of this prohibition is sanctioned under the criminal law. There were no instances in Slovenia for authorising by a national competent authority or EU making the funds available to persons and entities designated by PF TFS.

719. The competent authorities were not able to provide information on application of prohibitions in practice. The competent authorities do not gather and analyse such data on transactions rejected.

11.5. FIs, VASPs and DNFBPs understanding of and compliance with obligations

11.5.1 FIs and VASPs

720. FIs and VASPs demonstrated a solid understanding of their TFS obligations and the requirement to freeze the assets of designated individuals or entities. They primarily use automated screening tools, which are kept up to date with the latest UNSCR listings. FIs and VASPs have procedures and sufficient resources to manage potential matches and discard false positives.

721. Competent authorities have informed FIs and VASPs about the Sanctions Implementation Guidelines issued by the PCGRM. However, FIs and VASPs generally were not aware of prevalent PF evasion typologies and how their services can be exposed. None of the FIs/VASPs had a genuine PF-related TFS hit.

11.5.2 DNFBPs

722. DNFBPs generally demonstrate a low level of understanding of and compliance with obligations in relation to the implementation of PF-related TFS.

723. Most of the DNFBPs were familiar with the concepts of UNSCRs and sanctions screening obligations, except for casinos, the real estate entities, and DPMS. However, DNFBPs were unaware of Sanctions Implementation Guidelines issued by the PCGRM, their sanctions compliance checks were confined to verifying the name of the customer or the party directly involved in the transaction with the UN TFS as published online.

724. Many supervisors of DNFBP sectors agreed that the level of understanding of and compliance with obligations in relation to the implementation of PF-related TFS in DNFBP sector is limited.

11.6. Competent authorities monitoring and ensuring compliance with PF-related targeted financial sanctions

11.6.1 FIs and VASPs

725. BoS generally monitors the implementation of PF-related TFS within full scope on-site inspections. While BoS performs certain outreach measures in the form of publishing information, issuing guidance and providing training, these do not include PF-related TFS as a subject. Employees of the BoS also have not received a separate training on PF-related TFS.

726. Inspections conducted by BoS indicate that most FIs and VASPs are generally compliant with TFS obligations. BoS has not imposed any fines for infringement in relation to compliance with PF-related TFS.

727. Other supervisory authorities of FIs have not recorded any activities to monitor and ensure compliance with PF-TFS by the OEs under their supervision.

728. Competent authorities did not provide OEs with targeted guidance or outreach in relation to the implementation of PF-related TFS that would include prevalent PF evasion typologies.

11.6.2 DNFBPs

729. Competent authorities do not conduct a regular monitoring and ensuring compliance with PF-related TFS.

730. Competent authorities had not informed DNFBPs about the Sanctions Implementation Guidelines, which are available online. No other targeted guidance or outreach in relation to the implementation of PF-related TFS has been provided to DNFBPs.

731. Competent authorities did not provide OEs with targeted guidance or outreach in relation to the implementation of PF-related TFS that would include prevalent PF evasion typologies.

Annex A: TECHNICAL COMPLIANCE ANNEX

This section provides detailed analysis of the level of compliance with the FATF 40 Recommendations in their numerical order. It does not include descriptive text on the country situation or risks and is limited to the analysis of technical criteria for each Recommendation. It should be read in conjunction with the Mutual Evaluation Report.

This technical compliance review is a continuation of the mutual evaluation and follow-up process of the previous round and provides new analysis for Recommendations where the country has made legal, regulatory or operational framework changes since its last mutual evaluation (dated 2017) with five follow-up reports with technical compliance re-ratings (dated 2018, 2021, 2022 and 2023[26]) and Recommendations where there has been a change in the FATF Standards for which the country has not previously been assessed. The Recommendations under review are R.1, R.2, R.4, R.8, R.10, R.11, R.12, R.13, R.15, R.16, R.18, R.19, R.20, R.21, R.22, R.23, R.24, R.25, R.26, R.27, R.28, R.30, R.31, R.34, R.35, R.36, R.37, R.38, R.40. These recommendations are identified with the Recommendation heading in green text.

For Recommendations not under review, pre-existing information from the country's most recent assessments has been compiled for inclusion in this annex. Such Recommendations are marked with a footnote cross-referencing the date and source of the information (i.e. the country's most recent mutual evaluation or follow-up reports with technical compliance re-ratings).

Recommendation 1 – Assessing risks and applying a risk-based approach

Criterion 1.1

Slovenia concluded latest NRA in July 2025, using the World Bank methodology. The 2025 NRA is based on data from 2020 – 2023 and concludes that the overall ML risk remains medium low and TF risk is low.

Criterion 1.2

The Slovenian Government is required to establish a permanent interministerial working group to carry out a national risk assessment of ML/TF (APMLTF-2, Art. 13).

In 2014 the Decision on the Establishment of the NRA Working Group established the Interdepartmental Group for Execution of the NRA for ML/TF and describes the following duties: performing the NRA; preparation of the report on ML/TF risks; preparation of the action plan on the basis of the findings of NRA; performing of other analyses in the field of ML/TF 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.

Criterion 1.3

Slovenia is required to complete an NRA every 4 years (APMLTF-2, Art. 13(1)). The previous NRA was completed in 2021 for data relating to 2016-2019, and adopted in February 2021. The latest NRA was adopted in July 2025 for data relating to 2020-2023.

Criterion 1.4

The OMLP is required to publish an NRA summary and any subsequent updates. However, there are no

26. Two follow-up reports adopted in May 2023 and December 2023.

established and/or formalised mechanisms for the dissemination directly to all stakeholders (APMLTF-2, Art. 14(1)).

Criterion 1.5

(a) Slovenia has some analysis on PF risks in its 2025 NRA but this is not sufficient to constitute a proper identification and assessment of PF risks.

(b) Art. 13 of the APMLTF-2 requires the Government to establish a permanent interministerial working group to carry out a national risk assessment of ML/TF. However, there is no mention of PF.

(c) Art. 13(1) of the APMLTF-2 requires Slovenia to complete an NRA every 4 years. However, this does not cover PF.

(d) Art. 14(1) requires OMLP to publish an NRA summary and any subsequent updates. However, there are no other legal provisions for the dissemination directly to all stakeholders.

Criterion 1.6

Art.14 of the APMLTF-2 provides for the purpose and use of the NRA. This includes improving the national regime for detecting and preventing of ML/TF including by identifying sectors or activities in which obliged entities apply stricter measures regarding customer screening and other obligations under this Act; prioritising resources and assets aimed at preventing ML/TF, and reporting on national efforts as well as on human and financial resources dedicated to combating money laundering and terrorist financing (APMLTF-2, Art. 14(2)).

Criterion 1.7

One of the purposes of the NRA is to identify sectors or activities with a negligible or increased ML/TF risk (APMLTF-2, Art. 14).

Slovenia published a Decree on the exemption of organisers of classic games of chance from the implementation of AML/CFT measures which was rated as low risk in the NRA (APMLTF-2, Art. 9 and Art. 190(2)). The adoption of the Decree was based on a specific risk assessment conducted by the FARS in cooperation with the OMLP.

In the Gaming Act, games of chance include numerical lotteries, lotteries with currently known winnings, quiz lotteries, raffles, lotteries, sports predictions, sports betting, lotteries and other similar games. Classic gambling can only be organised occasionally to a very limited extent by non-profit humanitarian organisations and societies and are fully exempt from the implementation of AML/CFT measures. Any classic game of chance that is permanently provided can only be organised based on a concession granted by the Government, and the concession contract is concluded by the minister responsible for finance. Operators who permanently provide classic gambling services based on a concession by the Government, are partly exempted from measures relating to CDD, which must be implemented in accordance with the Decree.

Slovenia allows specific exemptions from the application of AML/CFT measures for legal entities, sole traders and self-employed persons (APMLTF-2, Arts. 4(1)(15), 4(19)(a)-(g)) who carry out financial activities on an occasional basis, ancillary and directly related to their main activity when there is proven low risk and subject to certain conditions (Art. 11 APMLTF-2). The above-mentioned entities shall file OMLP for application, demonstrating their compliance and low ML/TF risks. Art. 27 of the APMLTF-2 also allows for the suspension of CDD measures for certain e-money products when a risk assessment proves there is low ML/TF risk

Criterion 1.8

(a) There is enhanced CDD in cases of correspondent banking relations, for PEPs, or when a customer or transaction is related to a high risk third country (APMLTF-2, Art. 64). Obliged entities also take enhanced measures when an increased risk has been identified in the NRA (APMLTF-2, Art. 64(2)).

(b) Obliged entities are required to take into consideration the NRA and the EU supranational risk assessment, when establishing their own risk assessment (APMLTF-2, Art. 18(7)).

Criterion 1.9

Obliged entities are permitted to apply simplified CDD (APMLTF-2, Arts. 62 and 63) provided that lower risks are identified, including where the NRA identifies sectors or activities with minor ML/TF risks (APMLTF-2, Art. 14(2)2). *Reference is made to the analysis of relevant criteria in R.26 and R.28 for further details on the structural and substantial elements of the AML/CFT supervisory and control regime in Slovenia.*

Criterion 1.10

Supervisory authorities are responsible for ensuring compliance by all FIs and DNFBPs with the APMLTF-2, which includes implementing obligations stated within R.1 (APMLTF-2, Arts. 152-155).

Criterion 1.11

Slovenia has conducted some analysis of PF risks, which is included in its 2025 NRA. However, Slovenia does not have any legal provisions regarding PF risk mitigation. All provisions noted in criteria above refer only to ML/TF.

Criterion 1.12

Obliged entities are required to assess ML/TF 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 (APMLTF-2, Art. 18). This includes (a) documenting their risk assessment (APMLTF-2, Art. 18(2)-(8)), (b)considering all relevant risk factors (APMLTF-2, Art. 18(2)-(5)), (c) requiring obliged entities to update their risk assessment at least every 2 years (APMLTF-2, Art. 18(8)), and (d) the provision of the risk assessment to the relevant supervisory authority upon request (APMLTF-2, Art. 18(8)).

Criterion 1.13

(a) Obliged entities are required to establish effective policies, controls and procedures, in proportion to their activity and size, to effectively mitigate and manage identified risks of ML/TF (APMLTF-2, Art. 20). Prior to the introduction of policies, controls and procedures, obliged entities shall obtain the approval of their own management.

(b) There are requirements for medium-sized and large obliged entities to monitor the implementation of AML/CFT controls, however there are no obligations on other type of entities, Furthermore, there are obligations for any OEs to enhance them when necessary (APMLTF-2, Art. 20(2)).

(c) If an obliged entity considers that a customer, business relationship, transaction, product, service, distribution channel, country or geographical area poses an increased risk of ML/TF, it shall implement enhanced CDD measures (APMLTF-2, Arts. 19, 64-70).

Criterion 1.14

Obliged entities may apply simplified CDD in a number of cases (APMLTF-2, Arts. 62-63), however this is not permitted if reasons exist to suspect ML/TF in relation to a customer, transaction, property or assets (APMLTF-2, Art. 62(5)).

Criterion 1.15

Slovenian authorities have advised that PF risks are addressed by FIs and DNFBPs within the framework of existing TFS and compliance programmes. However, the AT has not been provided any evidence to demonstrate compliance with this criterion.

Weighting and Conclusion

Slovenia has measures in place for ML/TF risk mitigation, with obliged entities having policies, controls and procedures to effectively mitigate, monitor and manage ML/TF risks. However, there are significant gaps in relation to identifying, assessing, and understanding PF risks. **R.1 is rated PC.**

Recommendation 2 - National Co-operation and Co-ordination

Criterion 2.1

Art. 13(2)(3) APMLTF-2 states that the NRA Inter-agency working group is in charge of preparing an Action Plan. An action plan was adopted in 2021, following the adoption of the 2021 NRA. However, even though the interministerial working group identified that the action plan required to be more detailed and updated, this has not yet been actioned. The 2021 action plan remains in place and is supplemented by a new action plan adopted following completion of the 2025 NRA.

Certain elements of AML/CFT prevention, coordination and cooperation are included in the "Resolution on National Program of preventing and fighting against Crime 2019–2024 and 2024-2028" (adopted in 2019 and 2024 respectively). These documents allocate responsibilities among competent authorities in tackling cybercrime, organised crime, TF, seizure and confiscation.

Furthermore, there are no provisions with respect to PF.

Criterion 2.2

The OMLP, supervisory authorities and competent AML/CFT authorities cooperate and coordinate the implementation of policies and activities to combat ML/TF (APMLTF-2, Art. 12). To achieve the strategic and operational objectives, the competent authorities may conclude cooperation agreements and set up interministerial working groups. The OMLP performs AML/CFT tasks and any other tasks, which includes the authority to propose to the competent authorities changes and amendments to regulations concerning the prevention and detection of ML/TF and directing and coordinating the work and tasks of the permanent inter-ministerial working group established to carry out the NRA (APMLTF-2, Arts. 152-155). However, the scope of the inter-ministerial working group does not extend to the cooperation, coordination and exchange of information concerning the development and implementation of AML/CFT policies, by policy makers, the FIU, law enforcement and supervisors.

There are several working groups established for the cooperation, coordination and exchange of information (e.g., for restrictive measures, counterterrorism, and cooperation between the Police, State Prosecutor's Office, and competent authorities). However, this is for operational purposes and not for ML/TF policies or strategies.

Criterion 2.3

The OMLP and relevant supervisory bodies are required to work together to perform their tasks and exercise their powers in relation to supervisory activities (APMLTF-2, Art. 170). To achieve this goal, supervisory authorities may sign agreements on mutual cooperation and establish inter-ministerial working groups to attain both operational and policy level goals. The "Resolution on National Program of preventing and fighting against Crime 2024-2028" defines activities that have to be performed by state and, in some cases, international authorities.

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 ML/TF was set up in 2012. Although the AT has not seen this document, 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 ML/TF; and compare Slovenian legislation and court practice with those of other countries.

The Slovenian Government established an Interdepartmental Group for Execution of the NRA in 2014 (chaired by the OMLP) responsible for carrying out a ML/TF NRA and an action plan for mitigating the identified ML/TF risks (APMLTF-2, Art. 13).

Slovenia has advised that PF is considered within the context of restrictive measures, however, there are no specific provisions with respect to PF.

Criterion 2.4

Slovenia implemented a Regulation on cooperation between the public prosecutor´s office, the police and other competent state bodies and institutions in the detection and prosecution of offenders and the operation of specialised and joint investigations teams. This Regulation is limited as 1) it only relates to criminal investigations, 2) it only provides powers to the public prosecution to obtain information and 3) obliges the police to provide specified information to the public prosecution. The Regulation does not provide for the cooperation and coordination of information across all competent authorities. The Police have also concluded agreements on mutual cooperation and exchange of information with other state bodies and institutions, such as, with the OMLP and the Court of Auditors relating to the use of public funds, with the Ministry of Interior on corruption related matters, with the FARs on the prevention, detection and investigation of criminal offences, and with the Bank Association relating abuses of electronic banking.

The SMA advised it holds a number of cooperation and exchange agreements with other competent authorities, although the AT was not provided with these agreements to consider their compliance with this recommendation.

Furthermore, see c.29.5 with respect to the information that the OMLP shares with competent authorities. Additionally, the OMLP has signed a cooperation agreement with the BoS.

Slovenia has not demonstrated there are any other formal mechanisms for the operational co-operation and coordination between competent authorities.

Criterion 2.5

Art. 24 of the national Data Protection Act (ZVOP-2) requires for the Information Commissioner to be consulted on all laws containing provisions on the processing of personal data. This includes the implementation and revisions to APMLTF-2. The Information Commissioner has also provided an opinion in 73 cases on the processing of personal data in procedures relating to ML/TF.

Weighting and Conclusion

Slovenia has some inter-agency frameworks and mechanisms in place for co-operation and co-ordination, but there are moderate deficiencies as these do not apply to all relevant agencies and competent authorities and do not cover all the topics such as PF. **R.2 is rated PC.**

Recommendation 3 - Money laundering offence

In its 2017 MER, Slovenia was rated LC with R.3 based on the following deficiencies: the act of ML in the form of simple possession and use of property was not criminalised and the scope of certain ancillary offences. Since then, Slovenia has not amended relevant provisions in the context of R.3 and thus, the below analysis represents a summary of 2017 MER findings.

Criterion 3.1

ML is criminalised with almost all elements of the Vienna and Palermo Convention incorporated into legislation, except possession and use of proceeds of crime (CC, Art. 245 and 217).

Criterion 3.2

Slovenia applies all crime approach. Almost all deficiencies in the incrimination of TF offence have been rectified (see the 2023 FUR).

Criterion 3.3 (Not applicable)

Criterion 3.4

ML offence as criminalised in Art. 245 of CC is broad enough to cover all types of property, since there are no specifications.

Criterion 3.5

It is not necessary that a person is convicted of a predicate offence when proving that property is the proceeds of crime.

Criterion 3.6

Predicate offences for money laundering are extended to conduct that occurred in another country, which constitutes an offence in another country, and which would have constituted an offence had it occurred domestically.

Criterion 3.7

Self-laundering is provided for in general terms and criminalised under Art. 245 (2) CC. However, self-laundering in relation to simple acquisition, possession or use of proceeds of crime is not covered due to the fundamental principles of domestic law.

Criterion 3.8

In Slovenia, the principle of free evaluation of evidence applies (CPA, Art. 18) and it is used to ensure that when proving ML offence, the intent band knowledge of the perpetrator can be inferred from the objective factual circumstances. See the 2017 MER.

Criterion 3.9

The applicable sanctions for ML offense are proportionate and dissuasive (CC, Art. 245).

Criterion 3.10

Legal entities can be held criminally liable for offences, including ML (CC Art. 42 and Liability of Legal Persons for Criminal Offences Act (LLPA), Art. 5(2). 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.

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

R.3 is assessed as LC

Recommendation 4 - Confiscation and provisional measures

The FATF Standards for R.4 have undergone a revision against which the country has not previously been assessed. On this basis, R. 4 is regarded as a recommendation under review (RUR).

Criterion 4.1

(a) From the policy perspective Supreme State Prosecutor issued 2024 Law Enforcement Policy obliging prosecutors to give priority to asset recovery, and Ministry of Interior (MoI) issued policy addressing the issue of tracing and seizing of assets as priority. There is, however, no overarching policy which would target prioritisation of asset recovery issues in both domestic and international context.

On the operational level, in both Police and Prosecutor's office there are specialised stuff dedicated to asset recovery issues, nevertheless there is a lack of resources.

(b) The SPO's policy cited above includes a general requirement for instructions in the policy to be monitored and updated or supplemented when necessary. However, the same cannot be stated for the MoI's policy.

(c) The SPO has a dedicated central unit, the Expert Information Centre (EIC) that offers advice to State Prosecutors, provides expert assistance, co-ordinates co-operation in regard to confiscation and retains a centralised record of proposals and orders. However, the EIC is not sufficiently resourced. The sufficiency of resources within the wider regime, particularly those competent authorities tasked with financial investigations, local Prosecutors and the judiciary is also not sufficient.

(d) The role of the SPO as the primary authority responsible for initiating asset recovery provides a consistent domestic framework. The SPO sets guidelines for police work, the work of joint investigation teams, and other authorities, including the OMLP (CPA, Art. 160 (a and b) and ACIOP, Art. 13). There is a precedent for cross agency working groups tasked with enhancing co-operation and co-ordination, such as the that consisting of the he Police, State Prosecutor's, the FIU and other institutions (Anti-Corruption Commission, SMA, FARS) and their focus includes asset recovery issues.

Criterion 4.2

(a) The court conducting criminal proceedings and other relevant authorities gather evidence and undertake investigations when determining the proceeds of criminality, including property of corresponding value (CPA, Art. 499 and CC, Art. 75). Financial investigations are carried out by the prosecutors in the event that there are grounds for suspicion that a person has assets of illicit origin (ACIOP, Art.3). In addition the court assesses the amount of the proceeds of crime (CPA, Art. 499 and 500).

(b) Investigators are permitted to use a range of investigative measures specified in the CPA, including securing and gathering evidence by compulsion in order to obtain the data and evidence necessary to secure confiscations of the proceeds or associated proceeds of crime (CPA, Chapter 15 and 16 and Art. 12(1) of ACIOP). However, deficiencies identified under c. 31.1 have a cascading effect.

Criterion 4.3

(a) The OMLP is authorised to issue a written order, or in limited circumstances orally, temporarily suspending a transaction if there are reasonable grounds to suspect a criminal offence of money laundering or terrorist financing (APMLTF-2, Art. 105). The provisions of Art. 105 do not extend to predicate offences.

(b) The OMLP may suspend a transaction for a maximum of 72 hours (3 business days) to facilitate further enquiries.

Criterion 4.4

(a) In criminal investigations and criminal proceedings, competent authorities can seize goods gained, used or intended for use in criminality, if they are the perpetrator’s property or where they are not the perpetrator’s for reasons of general security or morality and if the rights of other persons to claim damages from the perpetrator are not thereby affected (CC, Art. 73(1) and CPA, 502(1 and 3)). Property of corresponding value may be seized (CPA Art. 502(3) and CC. Art. 75(2)). In civil forfeiture, the court may also order temporary measures to secure the assets of illicit origin upon the motion of the SPO and in relation to specified assets, where there is a serious risk of de-valuation, further use in criminality or used in a manner to frustrate forfeiture (ACIOP, Art. 20, 21 and 24).

(b) Initial seizure of criminal property can be done ex-parte and without notice as this measure intended to facilitate a challenge from the effected parties only after the order has been granted (CPA, Art.502a (3) & (5)).

(c) An application to the court to temporarily secure assets are not unduly restrictive and provide a safeguard to those potentially affected by an order, in instances where applications are made without notice (CPA, Art.502 (1) and ACIOP, Art. 20(1)).

Criterion 4.5

Competent authorities do not have legal possibility to freeze and seize criminal property and property of corresponding value without a court order when it is necessary to act expeditiously (CPA, Art.502).

Criterion 4.6

Competent authorities can take steps to prevent or void actions that prejudice their ability to freeze, seize or recover property subject to confiscation, including provisions to prevent the dissipation and concealment of property. Property held by third parties or close relatives can be seized (CC, Art.75 (3 and 4)) as well as property held by 3rd parties that the offender had exclusively or mostly used for their own benefit (CC, Art.77 (b) and (c)). Furthermore, under civil forfeiture, assets of suspected illegal origin are subject to a presumption of gratuitous transfer if it is transferred to closely related parties or immediate family members of the offender (ACIOP, Art.6). Also, the reverse burden of proof is applied to closely related parties or immediate family members when property has been transferred to them in order to avoid confiscation (ACIOP, Art. 27).

Criterion 4.7

Slovenia has legislative measures to enable the confiscation of money, valuables and other proceeds obtained from a criminal offence or assets of a corresponding value from the perpetrator or recipient as criminal proceeds (CC, Art.75(1)), subject to a court decision establishing the existence of a criminal offence (CC.

Art.74(2) and Art.75(2)).

Criterion 4.8

The authorities are able to confiscate property held by a criminal or criminal organisation that may not be directly linked to a specific crime, but which can be inferred derive from criminal conduct (CC, Art.77(a) to (c)).

The ACIOP details further procedures for extended confiscation. The court is able to make an assumption that assets held by a Suspect, an Accused Person, a Convicted Person or a Testor (estate of a deceased person) originate from criminal conduct (ACIOP, Art.5). Specifically in circumstances where there are reasonable grounds to suspect that they have committed a listed offence including ML and TF.

Criterion 4.9

The court can undertake non-conviction-based asset seizure and recovery, with the burden of proof reversed onto the property owner (ACIOP, Art.5 & Art.27).

Criterion 4.10

The competent authorities are able to cooperate, coordinate and share information domestically in order to support identification of criminal property and with the view to enhance assets recovery efforts. These measures are available in criminal proceedings and civil forfeiture (CPA, Art. 160 (a), ACIOP, Art. 5(2), 8(2), 10, 14 and 20).

Criterion 4.11

Slovenia has mechanism in place for the management, preservation and disposal of frozen, seized and confiscated assets. The court are required to act as a good manager and in an expeditious manner (CPA, Art. 506a (1)) with the possibility of pre-sale or donation, should the property risk devaluation or dis-proportionate costs (CPA, Art. 506a (2)). These general provisions are furthered elaborated by the Decree on the management procedure applied to seized items, assets and securities regulations for the management (2012). For the assets seized within the framework of civil forfeiture, there are defined bodies responsible for the secure storage and management of both assets temporarily secured or forfeited, and those forfeited (ACIOP, Art.37). The legislation (ACIOP, Art. 39-41) makes further reference to relevant regulations detailing management, realisation, payment, and costs of asset management. These bylaws include Decrees on the records of forfeited assets of illicit origin (2012) and the procedures of safekeeping, management and sale of assets of illicit origin (2012).

Criterion 4.12

The authorities are able to enforce confiscation orders and realise the property or value (CPA, Art.131).

Criterion 4.13

(a) Within the criminal proceedings, the court shall decide on the return of confiscated property to its legitimate owner (CPA, Art.100 (2) and 106). The return of property to the injured party may be authorised prior to the completion of the criminal proceedings in instances where the property is not being used as evidence, ownership is not being contested by other parties and has been established (CPA, Art.110).

(b) the confiscated property may be used to compensate victims. Pecuniary claims for compensation for the damage(s) arising from criminality may be submitted in the criminal procedure. The court will adjudicate on the claim having given the accused person an opportunity to respond to the claim(s) (CPA, Art. 100 (2-4). Priority is given to an injured parties claim for damages over confiscation, which can only be ordered where the value of the proceeds exceeds the adjudicated claim (CC, Art.76 (1)).

Individuals with pecuniary claims may in the alternative seek to recover property in full or part by means of civil proceedings, including in circumstances where a criminal court has either declined the claim or made a partial awarded. Civil litigation includes potential claims for damages arising from confiscated property

Weighting and Conclusion

Slovenia has some legislation and a framework that allows for both conviction and non-conviction-based confiscation. Nevertheless, there are major deficiencies identified including: lack of overarching asset recovery policy, no comprehensive periodic review of the asset recovery regime, lack of resources and no legal power to suspend transaction in relation to predicate offence as well as to freeze and seize criminal property without court order. **R.4 is rated PC**

Recommendation 5 - Terrorist financing offence

In its 2017 MER, Slovenia was rated PC with R.5 on the bases of the major deficiencies in the incrimination of TF offence, since it did not cover financing of all offences required by the TF Conventions. In the 2023 follow-up process, R.5 was upgraded to LC given that majority of the deficiencies were addressed. Slovenian authorities reported that there were no changes introduces since the 2023 FUR.

Criterion 5.1

TF offence is mostly criminalised on the bases of the TF Convention (CC, Art. 109); However, it does not fully cover financing of all the offences in the treaties listed in the Annex to the FT Convention.

Criterion 5.2

TF offence extends to provision or collection of funds or other assets, directly or indirectly with the intention to be used in full or in part to carry out terrorist act or by terrorist organisation or by an individual terrorist even without link to specific terrorist act (CC, Art. 109 (3)). A broad interpretation of TF offence is confirmed by the authorities.

Criterion 5.3

CC criminalises the travel for the purposes of perpetration and participation (CC, Art.108), planning and preparation (CC. Art. 108(3)) as well as providing or receiving terrorist training (CC, Art. 111). The financing of these acts is criminalised by Article 109 CC.

Criterion 5.4

The wording of TF offence does not specify a source of money or property, so it can be concluded that it refers to any funds or other assets whether from legitimate or illegitimate source.

Criterion 5.5

TF offence does not require that the funds or other assets were actually used nor that they should be linked to specific terrorist acts (CC, Art. 109 (2)).

Criterion 5.6

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 would enable judges to make such inference (CPA, Art. 18).

Criterion 5.7

The applicable criminal sanctions in cases of conviction for TF offence are proportionate and dissuasive (CC, Art. 109, 49 and 74).

Criterion 5.8

Legal persons may be held criminally liable for TF offence independently of the liability of natural or responsible persons, with available sanctions that appear proportionate and dissuasive.

Criterion 5.9

There are appropriate ancillary offences to the TF offence, including attempt, participation as an accomplice and organising or directing others (CC, Art. 20 and 34). Art. 294 CC prescribes the offence of participation in a criminal association.

Criterion 5.10

TF is a predicate offence for ML. Slovenia uses an "all crimes approach" for ML.

Criterion 5.11

Pursuant to the general provisions of the CC on jurisdiction (CC, Art. 10 – 14), the TF 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

Slovenia's CC does not fully cover financing of all the offences in the treaties listed in the Annex to the FT Convention (c.5.1). Nevertheless, Slovenia has fully covered all other important requirements under R.5. R.5 is rated LC

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

In its 2017 MER, Slovenia was rated PC with R.6, based on the following deficiencies: the delays in the implementation of targeted financial sanctions (TFS) due to the overreliance on EU framework; an absence of explicit procedures at the national level in relation to proposing designations to UNSC Committees; a lack of awareness about TFS among DNFBPs and some FIs; an absence of national procedures for unfreezing requests; and a lack of publicly known national procedures for delisting requests. In its 2021 FUR, Slovenia addressed most of the identified deficiencies and R.6 was re-rated as LC.

Since then, Slovenia amended the Act on Restrictive Measures Introduced or Implemented by the Republic of Slovenia in Accordance with Legal Acts and Decisions Adopted Within the Framework of International Organisations (RMA), Rules of Procedure of the Permanent Coordination Group for Restrictive Measures (PCGRM RoP) and published a new Guidelines for the effective implementation of restrictive measures (RMG). These changes are considered material. On this basis, R.6 is regarded as a RUR.

Slovenia implements TF TFS through EU decisions and regulations, complemented by domestic legislation.[27]

27. At the EU level UNSCR 1267/1989 (on Al Qaida) are implemented through Council Decision 2016/1693/CFSP and EU Regulation 881/2002; UNSCR 1988 (on Taliban) – through Council Decision 2011/486/CFSP and EU Regulation 753/2011; and the UNSCR 1373 - through Council Common Position (CP)2001/931/CFSP and EU Regulation 2580/2001.

Criterion 6.1

(a) The Ministry of Foreign and European Affairs (MFEA) is the responsible authority for proposing the persons or entities to the 1267/1989 and 1988 Committees for designation (Foreign Affairs Act (FAA), Art. 2(1); RMA, Art. 6(3); PCGRM RoP, Annex I, para. 36) Designation proposal is made: (a) either on the basis of a national designation by the Government upon proposal of the coordination body in charge of monitoring and coordinating the implementation of restrictive measures, which is the Permanent Coordination Group on Restrictive Measures (PCGRM), or (b) upon decision of the PCGRM (RMA, Art. 3-4; Government decision on establishing PCGRM, Art.2(1); PCGRM RoP, Annex I, para. 36).

(b) Slovenia has a mechanism – PCGRM, Sanctions Coordination Group - for identifying targets for designation, based on the designation criteria set out in the relevant United Nations Security Council resolutions (UNSCRs) (PCGRM RoP, Annex 1, Chapter II).

(c) PCGRM should base its decision upon designation proposal on the requirements and criteria set for relevant UNSCRs. Therefore, such proposals for designations are not conditional upon the existence of a criminal proceeding (PCGRM RoP, Annex 1, Chapter II).

(d) The PCGRM should follow relevant UNSC procedures, including the use of appropriate templates or forms when proposing a designation (PCGRM RoP, Annex 1, Chapter II).

(e) Slovenia shall follow the UN legal acts and the procedures when proposing a listing (PCGRM RoP, Annex1, Chapter II). Decision on making the status of Slovenia know as designating state may be known is to be decided on a case-by-case basis.

Criterion 6.2

(a) At the EU level, the EU Council (through the Council's Working Party on the Application of Specific Measures to Combat Terrorism (COMET)) is responsible for designating persons or entities that meet the criteria set forth in UNSCR 1373. Designations are considered based on proposals submitted by EU member states or third states. (EU Regulation 2580/2001, Art. 2(3); CP 2001/931/CFSP, Art. 1(4)). Relevant designations of EU internals (i.e., natural persons who have their roots, main activities, and objectives within the EU) only trigger enhanced police and judicial cooperation. (CP 2001/931/CFSP footnote 1 of Annex 1).

At the national level, the Government of Slovenia is the competent authority for domestic designation of persons or entities, upon proposal of the PCGRM. PCGRM is the responsible coordination body in charge of monitoring and coordinating the implementation of restrictive measures. Criteria set out in UNSCR 1373 shall be used when deciding upon designation. Slovenia may designate persons or entities on its own motion, on the basis of the PCGRM member proposal and request of another country - EU Member State or a third country. (PCGRM RoP Annex 1, Chapter I (para-s 4 and 6) and Chapter II (para-s 1 and 2).

(b) At the EU level, proposals for listings are made by member states (for proposals based on decisions taken by their own competent authorities), or by member states or the High Representative for Foreign Affairs and Security Policy (HR) for proposals on the basis of decision(s) by third States' competent authorities. The EU (through COMET) applies designation criteria consistent with the designation criteria of UNSCR 1373 (CP 2001/931/CFSP, Art. 1(2) and (4); CR 2580/2001, Art. 2 (3), COMET mandate, practical arrangements and working methods 10826/1/07 REV`1).

At the national level, within the PCGRM the Sanctions List Sub-Group is tasked with identification of persons or entities for designation and preparing the proposal. Sanctions List Sub-Group should consider whether the criteria set out in UNSCR 1373 are met. Sanctions List Sub-Group submits a written proposal for a listing opinion, giving reasons for each listing, to the PCGRM for adoption. Once adopted, the MFEA shall submit the proposal to the Government for approval by means of adoption of a Regulation on designation. (RMA, Art. 3(1); PCGRM RoP, Annex1, Chapter I (para-s 4-22) and Chapter II (para-s. 1-2).

(c) At the EU level, the European External Action Service or relevant member state (acting as intermediary) when receiving a request for designation from a non-EU country, will carry out a first basic scrutiny of the proposal and gather relevant information, including requesting additional information from the requesting country, in particular with regard to and respect for fundamental rights. (CP 2001/931/CFSP, art. 1(2) and (4), as well as COMET mandate, practical arrangements and working methods). If an EU country requests an EU designation, the compliance with due process is assumed when the EU reviews such requests. COMET has 15 days to review the proposal, this timeframe can be shortened in exceptional cases. (doc.14612/1/16 REV 1 on establishment of COMET, Annex II, arts.8-9).

At the national level, Sanctions List Sub-Group members have 15 calendar 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 Sanctions List Sub-Group must issue a written proposal together with a statement of reasons for designation proposal. Within 5 working days the PCGRM would adopt the designation. Within 5 working days the MFEA shall prepare the relevant legal act and submit to the Government. (PCGRM RoP, Annex1, Chapter I (para-s 13-19) and Chapter II (para-s. 1-2)

(d) At the EU level, when deciding on a proposal, COMET decides on the basis of a decision (and the information/material supporting that decision) by a competent national body, irrespective of criminal proceedings (CP 2001/931/CFSP, Art.1(4)).

At the national level, the PCGRM should base its decision upon designation proposal on the requirements and criteria set for UNSCR 1373. Therefore, such proposals for designations are not conditional upon the existence of a criminal proceeding (PCGRM RoP, Annex 1 Chapter I (para-s 6-7 and 9) and Chapter II (para-s. 1-2)).

(e) There is no EU procedure or requirements regarding the provision of identifying or supporting information with respect to requesting non-EU countries to give effect to EU designations. Information to support designation may be shared with non-EU members upon request provided EU member states agree.

At the national level, there is no procedure in respect of requesting third countries to give effect to 1373 designations and regarding information to be provided for identification, as well as specific information to support the decision.

Criterion 6.3

(a) At the EU level, all member states are required to provide each other with all available relevant information to identify persons meeting the criteria for designation (CP 2001/931/CFSP, Art. 4; EU Regulation 2580/2001, Art. 8; EU Regulation 881/2002, Art. 8).

At the national level, legal framework does not prescribe specific authorities or mechanisms to collect or solicit information to identify targets for designation. Once the Sanctions List Sub-Group received a proposal for designation, it may request additional information from the proposing party while conducting first basic screening of the proposal (PCGRM RoP, Annex 1, para. 4 and 9).

(b) At the EU level, designations take place without prior notice (EU Regulation 1286/2009, preamble para.5).

At the national level, the authorities can act *ex parte* against a person or entity who has been identified and whose proposal for designation is being considered. The MFEA informs the person or entity who has been designated, after a listing decision has been taken (PCGRM RoP, Annex 1, para 23).

Criterion 6.4

At the EU level, implementation of TFS, pursuant to UNSCRs 1267/1989 and 1988, does not occur "without delay."[28]

For TFS under the UNSCR 1373 mechanism, these measures are implemented without delay, except in respect of EU internals. New designations are published on the day they are adopted, and enter into force the same day. Once the decision to freeze has been taken, EU Regulation 2580/2001 is immediately applicable within all EU member states.

At the national level, UNSCRs on TFS issued in accordance to EU Regulation, apply from the date of the publication of the updated list on the UNSC website until the entry into force of the relevant amendment of annexes to EU Regulations, thereby partly closing the gap between the entry into force of TFS and the moment they are implemented in the EU law (Art. 3(4) of the RMA). Issues remain with EU internals.

As concerns implementation of TFS issued on the basis of the UNSCR 1373, those are issued by the Government by means of adoption of Regulations. These enter in effect and in force on the day following the publication.

Criterion 6.5

(a) At the EU level, for 1373 designations, there is no requirement to freeze assets of listed individuals that are EU internals. Listed EU internals are only subject to increased police and judicial cooperation among members (CP 2001/931/CFSP, footnote 1 of Annex 1).

Under UNSCRs 1267/1989, 1988, 1373 all natural and legal persons within or associated with the EU are required to freeze without prior notice and delay the funds or other assets of designated persons and entities. (EU Regulation 753/2011, Arts. 3, 14; EU Regulation 881/2002, Arts.2(1), 11; EU Regulation 2580/2001, Arts.2(1)(a), and 10).

At the national level, in addition to EU Regulatory framework, Slovenia specified a freezing requirement for public administration authorities, other public law entities and bearers of public authority (RMA, Art. 3(5)). There is no explicit requirement to freeze assets without delay and without prior notice. There are no additional freezing requirements set for natural and legal persons at the domestic level, hence UN designated EU internals will not be covered for the latter.

(b) At the EU level, freezing actions for UNSCRs 1267/1989 and 1988 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, or by a third party acting on their behalf or at their direction. This extends to interest, dividends or other income on or value accruing from or generated by assets (EU Regulation 881/2002, Arts.1(1), 2; EU Regulation 753/2011, Arts.1(a), 3). This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35).

Under the EU mechanism on UNSCR 1373, the freezing obligation applies to all funds, other financial assets and economic resources belonging to, or owned or held by the designated person or entity (EU Regulation 2580/2001, Arts.1(1), 2(1)). There is no explicit reference to funds or assets controlled by, indirectly owned by, derived from assets owned by, or owned by a person acting at the direction of a designated person or entity. However, this gap is largely addressed by the EC's ability to designate any legal person or entity

28. This is due to the time taken to consult between European Commission departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages. Though expedited procedures allow for implementation within 72 hours where possible, this does not meet the requirement of "without delay".

controlled by, or any natural or legal person acting on behalf of, a designated person or entity (EU Regulation 2580/2001, Art.2(3) (iii) and (iv)). As above, the notion of joint-ownership is not explicitly covered, although this interpretation is taken in non-binding EU Best Practices (EC document 8518/18, para.35).

At the national level, measures in respect of UNSCRs 1267/1989 and 1988, as well as UNSCR 1373 designations do not appropriately extend to all funds and other assets (including jointly-owned assets).

(c) At the EU level, natural and legal persons are prohibited from making funds, other assets or economic resources available unless authorised by a national competent authority (EC Regulation 881/2002, Art. 2(2), (3); EU Regulation 753/2011, Art. 3(2); EU Regulation 2580/2001, Art. 2(1)(b)). The EU UNSCR 1373 mechanism explicitly extends to the provision of financial services (EU Regulation 2580/2001, Art. 2(2)). While there is no similar explicit prohibition in the EU for the UNSCR 1267/1989 and 1988 mechanism, this is covered by the broad definition of funds and other assets (economic resources) and the prohibition to make available assets that can be used to obtain such services (EU Regulation 881/2002, Art. 1(2); EU Regulation 753/2011, Art. 1(c)). However, deficiencies in respect of freezing obligations noted under c.6.5(a) for EU internals applies to this criterion.

At the national level, breach of prohibitions by natural or legal persons is liable to punishment under misdemeanour (ARM, Art. 10a) and criminal law (CC, Art. 374a).

(d) At the EU level, information on EU designations is published in the Official Journal of the EU and included in the EU's Financial Sanctions Database the next working day (which includes a newsletter service to which FIs and DNFBPs can subscribe), though there may be delays to updates via the newsletter service notably in case of designations on Fridays or over the weekend. Guidance in relation to EU sanctions is published on the website of the EC.

At the national level, the MFEA shall publish on its website the link to UNSCRs (ARM, Art. 3(4)). Government Regulations on designations pursuant to UNSCR 1373 are published in the Official Journal. However, there is no domestic mechanisms in place to notify FIs and DNFBPs of UN and domestic designations immediately upon taking such action. Importance of following those publications by REs is communicated through trainings.

The PCGRM adopted a Guideline for the Effective Implementation of Restrictive Measures (RMG). This Guideline does not contain sector specific guidance for implementation of sanctions.

(e) At the EU level, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations to their respective national competent authorities. This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations. The scope gap in obligations in respect of 1373 designations (EU internals) also applies to this criterion. (EU Regulation 753/2011, art.8; EU Regulation 881/2002, art.5(1); EU Regulation 2580/2001, art.4).

At the national level, only FIs are required to report freezing of assets only under EU sanctions, to Bank of Slovenia (BoS). BoS shall in its turn report this to MFEA. Information to be reported is provided in the Regulation on the Database of Restrictive Measures (Art.3(4)). This falls short of requiring that all OEs report on frozen assets and actions taken on UN designated persons. The RMG give the specific contact details for the MFEA.

(f) At the EU level, for 1267/1989, 1988 and 1373 designations, third parties acting in good faith are protected (EU Regulation 753/2011, amended by EU Regulation 1286/2009, and 2016/1686 art. 12 and 13, art.6 and 7; EU Regulation 881/2002, art.6; EU Regulation 2580/2001, art.6).

At the national level, The RMA renders impossible compensation of damage caused through lawful implementation of sanctions (Art. 9).

Criterion 6.6

(a) At the EU level, for designations under the 1267/1989 and 1988 mechanisms, there are procedures to submit de-listing requests to the relevant UN Sanctions Committee in line with Committee procedures (EU Regulation 881/2002, Art. 7c; EU Regulation 753/2011, art.11(4)). EU measures imposing TFS pursuant to 1267/1989 and 1988 may be challenged by instituting proceedings before the EU Court of Justice (Art. 263(4) and Art. 275(2) of the Treaty on the Functioning of the European Union for challenging EU regulations or CFSP Decisions.).

At the national level, RMG advises on de-listing procedures for the persons designated by the UN Resolutions 1267/1989, and 1988. The document also contains a link to respective UN Committee website. (Section 1.2.7.2.).

(b) At the EU level, de-listing procedures are available for designations under the 1373 mechanism under EU Regulation 2580/2001.

At the national level, the RoP Annex does set out a procedure for delisting from the national list by the PCGRM. Requests can be made anytime by listed persons, groups and entities, by submission of supporting information to the MFEA, and will be discussed in the Group as a matter of priority (para. 31-34).

(c) At the EU level, a person or entities designated under the 1373 mechanism can write to the EU Council to have the designation reviewed by COMET (CP 2001/931/CFSP) or may institute a proceeding before the EU Court of Justice (Treaty on the Functioning of the European Union, Arts. 263(4), 275(2)).

At the national level, designated persons or entities can request a review of the designation decision before the Administrative Court (Administrative Disputes Act, Art. 5(4), RMG, Section 1.3).

(d) At the EU level, persons designated under UNSCR 1988 are informed of applicable de-listing procedures, which include the availability of the focal point (for designations under UNSCR 1988). (EU Regulation 753/2011, Art. 11(4)).

At the national level, for designations pursuant to 1988, the RMG refers to the UNSC Focal Point (RMG, Section 1.2.7).

(e) At the EU level, persons designated under UNSCR 1267 etc. are informed of applicable de-listing procedures, which include the availability of the UN Office of the ombudsperson (for UNSCR 1267/1989 designations). (EU Regulation 881/2002, art.7(a).

At the national level, for designations pursuant to 1267/1989, the RMG refers to the Ombudsperson (RMG, Section 4.1.2).

(f) At the EU level, procedures for unfreezing funds due to cases of mistaken identity are in place (EC document 8519/18, paras.8-17, 37).

At the national level, Slovenia does not to have publicly known procedures to unfreeze the funds of inadvertently affected persons.

(g) At the EU level, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c.6.5.d) also contains information on the obligations to respect a de-listing action.

At the national level, the MFEA shall publish on its website the link to UNSCRs (ARM, Art. 3(4)) and publishes a notice in the Official Journal (RMG, Section 1.2.7). Government Regulations on de-listing pursuant to UNSCR 1373 are also published in the Official Journal (ARM, Art. 3(3)). However, there is no domestic mechanisms in place to notify FIs and DNFBPs on UN and domestic de-listing and unfreezing immediately upon taking such an action. There is no specific guidance provided to FIs and DNFBPs on their obligations to respect a de-listing or unfreezing action.

Criterion 6.7

At the EU level, the regulations imposing TFS obligations contain measures for national competent authorities to authorise access to frozen funds, where necessary for basic expenses or the payment of certain expenses in line with UNSCR 1452 (EU Regulation 881/2002, Art. 2a; EU Regulation 753/2011, Art. 5; EU Regulation 2580/2001, Arts.5, 6).

At the national level, Slovenia has a procedure for granting authorisation to access frozen funds for basic and extraordinary expenses (RMG, Annex 1, Section 1.2.6). The Ministry of Finance would deal with such requests.

Weighting and Conclusion

Slovenia has established measures for implementation of UN TFS including through supra-national regulatory framework, but some minor shortcomings remain. These include: lack of procedures for requesting third countries to give effect to 1 373 designations; gap with application of measures to EU internals; lack of explicit requirement to freeze assets without delay and without prior notice; gap in application of measured to jointly-owned assets; issues with domestic mechanisms in place to notify FIs and DNFBPs of UN and domestic designations and de-listing immediately upon taking such action; no sector-specific guidance for REs on implementation of UN TFS measures, as well as lack of explicit requirement to report freezing of assets under UNSCRs. **R.6 is rated LC.**

Recommendation 7 – Targeted financial sanctions related to proliferation

In its 2017 MER, Slovenia was rated PC with R.7, based on the following deficiencies: the delays in the implementation of TFS; a lack of explicit coverage of TFS against proliferation financing (PF) in the guidance; an absence of guidance on freezing of assets for DNFBPs; a lack of publicly-known procedures for de-listing and unfreezing; an absence of mechanism for communicating de-listing and unfreezing actions to FIs and DNFBPs; and a lack of guidance for persons or entities on their obligations to implement a de-listing or unfreezing action. In its 2018 FUR Slovenia demonstrated no progress. In its 2021 FUR, Slovenia addressed most of the identified deficiencies and R.7 was re-rated as LC.

Since then, Slovenia amended the RMA, PCGRM RoP and published a new RMG. These changes are considered material. On this basis, R.7 is regarded as a RUR.

Slovenia implements PF TFS through EU decisions and regulations, complemented by domestic legislation.[29]

Criterion 7.1

At the EU level, implementation of TFS, pursuant to UNSCR 1718, does not occur "without delay." This is due to the time taken to consult between EC departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages.

At the national level, the regulatory framework and the identified gap as described under c.6.4 apply.

29. At the EU level, UNSCR 1718 (2006) on DPRK and its successor resolutions are implemented through Council Decision 2016/849/CFSP and EU Regulation 2017/1509.

Criterion 7.2

(a) At the EU level, all natural and legal persons within the EU are required to freeze the funds or other assets of designated persons or entities as soon as a designation is published, i.e. without prior notice (EU Regulation 2017/1509, Art.1 and 2). Though delays in implementation apply as described under c.7.1.

At the national level, the regulatory framework and the identified gap as described under c.6.5(a) apply.

(b) At the EU level, freezing actions for UNSCR 1718 extend to all funds and economic resources belonging to, owned, held or controlled, either directly or indirectly, by a designated person or entity, and includes assets generated from such funds. (EU Regulation 2017/1509, Art. 1 and 34). This does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35). While the definition does not explicitly cover funds or assets of persons acting on behalf or at the direction of a designated person or entity, this is largely captured by the coverage of funds 'controlled' by the designated person (Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, para 55b.).

At the national level, the regulatory framework and the identified gap as described under c.6.5(b) apply.

(c) At the EU level, EU nationals and natural and legal persons within the EU are prohibited from making funds and other assets available unless otherwise authorised or notified in compliance with the relevant UNSCRs (EU regulation 2017/1509, Art.34(3)). Regulations apply to any natural or legal person, entity, body or group in respect of any business done in whole or in part within the EU.

At the national level, the regulatory framework as described under c.6.5(c) applies.

(d) At the EU level, the same mechanism to communicate PF TFS is used as for TF TFS (see c.6.5(d)).

At the national level, the regulatory framework, set mechanisms and the identified gap as described under c.6.5(d) apply.

(e) At the EU level, all natural and legal persons (incl. FIs and DNFBPs) are required to report any information which would facilitate compliance with TFS obligations. (EU Regulation 2017/1509, art. 50). This requirement does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report "any information which would facilitate compliance" with the relevant Regulations.

At the national level, the same mechanism to report is used as for TF TFS (see c.6.5(e)).

(f) At the EU level, protections are in place for third parties acting in good faith (EU Regulation 2017/1509, Art.54).

At the national level, the regulatory framework as described under c.6.5(f) applies.

Criterion 7.3

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 RMA and in accordance with the regulations governing their individual supervisory fields (RMA, Art. 10). The 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 374a CC for the offence 'Violation of restrictive measures' (imprisonment between six months and five years).

Criterion 7.4

(a) At the EU level, listed persons are informed of their ability to petition the UN Focal Point or their own government for de-listing, through the EU Best Practices document for the effective implementation of restrictive measures (page 11, para. 23).

At the national level, RMG advises on delisting procedures for the persons designated by the UN Resolutions. Proposals for removal from the lists related to restrictive measures based on UNSC resolutions can be submitted directly to the relevant UNSC sanctions committee, through the UNSC focal point, or through the MFEA. (Section 1.2.7.2.).

(b) At the EU level, procedures for unfreezing funds due to cases of mistaken identity are the same as those described under c.6.6(f).

At the national level, Slovenia does not to have publicly known procedures to unfreeze the funds of inadvertently affected persons.

(c) At the EU level, the regulation imposing TFS obligations under UNSCR 1718 contains measures for national competent authorities to authorise access to frozen funds or other assets under the conditions set out in UNSCR 1718. (EU Regulation 2017/1509, Art. 35-36).

At the national level, the regulatory framework as described under c.6.7 applies.

(d) At the EU level, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. Guidance mentioned under c7.2(d) also contains information on the obligations to respect a de-listing action.

At the EU level, de-listings are communicated via publication of updated lists in the EU official journal and notifications within the EU sanctions database for subscribers. RMG mentioned under c.6.5.d) also contains information on the obligations to respect a de-listing action.

At the national level, the regulatory framework, set mechanisms and the identified gap as described under c.6.5(g) apply.

Criterion 7.5

(a) At the EU level, regulations permit the addition of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures. (EU Regulation 2017/1509, Art. 34(9)).

At the national level, there are no measures to ensure that there are equivalent provisions in any UNSCR 1718 mechanisms implemented domestically.

(b) This sub-criterion is not applicable, as the TFS elements of UNSCR 2231 expired on 18 October 2023. Therefore, this analysis did not assess the implementation of UNSCR 2231.

Weighting and Conclusion

Slovenia had established measures for implementation of UN TFS including through supra-national regulatory framework, but some minor shortcomings remain. These include: gap with application of measures to EU internals; lack of explicit requirement to freeze assets without delay and without prior notice; gap in application of measured to jointly-owned assets; issues with domestic mechanisms in place to notify FIs and DNFBPs of UN and domestic designations and de-listing immediately upon taking such action; no sector-specific guidance for REs on implementation of UN TFS measures, as well as lack of explicit requirement to report freezing of assets under UNSCRs. **R.7 is rated LC.**

Recommendation 8 – Non-profit organisations

In its 2017 MER, Slovenia was rated PC with R.8, based on the following deficiencies: a lack of identification of the types of NPOs which are likely to be at risk of TF abuse and related threats; an absence of targeted outreach to the NPO sector; a lack of best practices developed in cooperation with NPOs; an absence of effective supervision over NPOs, with the exception of associations; no requirement for foundations to keep up-to-date registered information on members of the Board of Trustees; no public access to founding acts of associations and foundations, as well as annual reports. In its 2021 FUR, Slovenia addressed most of the identified deficiencies and R.8 was re-rated as LC.

Since then, R.8 has undergone specific changes to clarify requirements under the FATF Standards regarding NPOs and the following criteria have been amended: c.8.1, 8.2(b)-(d), 8.3, 8.4(a) and 8.5(c). On this basis, R.8 is regarded as a RUR.

Criterion 8.1

(a) Slovenia conducted analysis for identifying the subset of NPOs that fall under the FATF definition within the scope of two exercises: Strategic Analysis of Risks Associated with the Abuse of Non-Profit Organisations for ML and TF in the Republic of Slovenia (NPO Strategic Analysis) in 2020 and the NRA in 2021. Slovenia advised that it is in the process of revising its analysis of the NPO sector, since the former analysis dates more than 4-5 years and hence do not reflect on the current situation.

NPOs in Slovenia can take different legal forms. Slovenia concluded that of those, only certain associations having a status of humanitarian organisations and certain foundations are considered to fall under the FATF definition since the other types are not primarily engaging in raising or disbursing funds. Humanitarian organisations (HO) are associations with a special status, granted by ministries in accordance with the Humanitarian Agencies Act. NPO Strategic Analysis concluded that there are 17 NPOs that potentially pose higher TF risk. The NRA 2021 does not reflect on the exact number of those. The ongoing analysis suggests that there are some foundations and some humanitarian organisations to potentially pose higher TF risk.

In addition, Slovenia assessed the risks of NPO abuse for TF in its 2025 NRA. While the analysis did not focus specifically on NPOs as defined by the FATF, it provided a general overview of the risk. The NRA found that TF threats are low in Slovenia but acknowledged a potential risk, particularly through NPO abuse. It also reviewed risks to financial institutions and DNFBPs serving NPOs and found no specific TF cases detected.

(b) The NRA identified a number of vulnerabilities that are pertinent to all NPOs in general but did not identify the risks of those individual NPOs and the nature of the TF risk posed on them. Among those are: a lack of a uniform supervisory authority; abuse of NPOs to commit criminal offences primarily related to ML; non-transparent sources of financing when NPOs are financed from abroad. The NPO Strategic Analysis advises that there are 17 NPOs which could potentially pose a TF risk, due to their international ties, countries of destinations and type of programs.

(c) Besides applicable legislation, Slovenia has not indicated the existence of any focused, proportionate and risk-based measures to address the TF risks identified in the NPO sector, in line with the risk-based approach. In addition, the NPO risk assessment identified a lack of measures to address TF risks in the NPO sector that could be developed by individual organisations or the sector and introduced in the organisations' operations (p. 21). At a general level, Slovenia advised to implement a Strategy for the development of Non-Governmental Organisations (NGOs) in the Republic of Slovenia 2018-2023 that includes a strategic goal of promoting transparency, integrity, and accountability of NGOs. As part of this goal, it proposes the preparation and implementation of educational programs and training.

Criterion 8.2

(a) Slovenia applies multiple mechanisms to promote accountability, integrity and public confidence in the administration and management of NPOs.

The associations are NPOs that shall operate publicly, be registered with the Register of Associations, have a charter, 1-2 representatives defined in the charter (natural person of contractual capacity); members of the association and the representatives shall be liable for Associations' operations; General Assembly shall be established to among others adopt the annual financial report of Association; Association shall perform bookkeeping, internal audit and external audit (if income or expenditure exceeds EUR 1 million); annual financial report shall be published (Associations Act, Art. 1-6, 9, 13 27, 29 and 50).

Associations can apply for obtaining the status of humanitarian organisations. They shall apply to a competent ministry and satisfy a set of requirements: prove to act for more than 1 year, present the proof of registration and present the act of association, demonstrate the that it independently disposes of funds and provide the work plan. Once the status is granted, a humanitarian organization conducts its financial operations in accordance with the accounting standards. It shall adopt an annual report on its operations and present it to the competent ministry, to donors and also publish the report. (Humanitarian Organisations Act Art. 22-37)

The foundations can be set up as generally beneficial or charitable organisations. Foundations shall be registered with a Foundation Register; have its rules and articles of association; governed by its board of trustees; ensure its bookkeeping; invite a certified audit; produce an annual report (Foundations act, Art. 5, 12, 13, 18, 21, 24, 27, 30, 33). Foundations are subject to additional reporting requirements to the competent ministry regarding their operations and financial management. The competent ministry may also request an external audit of their annual report (Foundations Act, Art. 30.) Foundations shall submit the annual financial reports (Accounting Act, Art. 51).

In line with Article 27 of the Foundations Act, foundations can accept the funds from donors. Nevertheless, there are no donor policies available in Slovenia.

(b) Within the framework of implementation of the Strategy for the development of Non-Governmental Organisations (NGOs) in the Republic of Slovenia 2018-2023 authorities reported to undertake educational programs and training initiative for promoting transparency, integrity, and accountability of NGOs. Slovenia has undertaken outreach to OEs and the NPOs on the targeted NPO risk assessment conducted in 2021 and the 2025 NRA. In addition, the CNVOS in cooperation with the OMLP and National Forum of Humanitarian Organizations of Slovenia conducted two conferences targeting the NPOs and the donor community covering subjects related to ML/TF risks and transparency matters.

(c) Slovenia maintains a dialogue with the non-profit sector, and exchange on best practices through various means and channels. Considering the financial and operational transparency as one of the ways to preventing the TF abuse of NGOs, as part of the NGOs' support environment, which is co-financed by the MPA in accordance with the Strategy for the Development of NGOs, 12 regional hubs carried out a joint campaign to increase NGO transparency in 2022. This resulted in a greater transparency of data on financial activities of those. In addition, the CNVOS promotes the transparent and responsible operations of organisations through the assessment tool published on its website. It includes a criterion for evaluating financial the flows of organisations.

(d) The NPOs are setup as legal persons in Slovenia therefore the requirement that the transactions need to be made through transaction accounts opened with payment service providers (Tax Procedure Act, Art. 36(1)) apply to them. The threshold on cash transactions applies. Below threshold transactions can be executed in cash.

Criterion 8.3

(a) and (b) Slovenia has a decentralised system of supervision over the work and financial operations of NPOs which is entrusted to various ministries in accordance with their respective competences. Competent authorities conducting supervision over the Associations are the Ministry of Interior (registration, distribution of funds), Tax Administration (accountancy and taxes), Agency for Public Records and Services (annual reports and publication (Associations Act, Art. 10, 20, 23, 24, 26 – 29, and Article 51). Supervision of the legality of intended purpose and efficiency of the use of public funds by a humanitarian organisation is carried out by its competent bodies and the Court of Audit of the Republic of Slovenia. Supervision of the use of allocated funds, the implementation of social programs and investments is carried out, in addition to the competent bodies of the humanitarian organisation, also by the financiers who have specifically allocated funds to the humanitarian organisation (Humanitarian Organisations Act, Art.38). Competent authorities conducting supervision over the Foundations the ministry whose operating range covers the purpose for which the foundation was established (supervising compliance with the provisions of Foundations Act, violations of which are defined as offences by this Act and (Foundations Act, Art. 30 and 30a). The oversight and monitoring measures are rule-based, and hence not focused, proportionate or risk-based. Measures are applied regardless of TF risk to all NPOs operating in the country.

Criterion 8.4

(a) According to Table 13 of the NPO risk assessment, 166 inspections were conducted in 2017 and 546 in 2018. However, no relevant information about the oversight of NPOs since 2018 has been made available to the AT. Measures are applied regardless of TF risk to all NPOs operating in the country.

(b) Societies Act provides for a fine from 420 to 16 500 euros for a misdemeanour by an association that does not keep business books in accordance with the provisions of Art. 26 or falsely presents data on financial and material operations. The responsible person of the association is also fined from 42 to 1 000 euros for the offense (Article 52). A fine of 420 euros shall apply to an association that has stipulated in the basic act that it will regulate the method of providing data on its financial and material operations in a special act, but does not regulate this, and an association that does not submit the annual report within the AJPES deadline, or does not attach an auditor's assessment to the annual report, when required. The responsible person of the association is also fined for this offense with a fine of 125 EUR (Art. 53). Foundation Act provides for fines for illegal operation, non-registration of changes, breaching the rules of foundations, failure to submit reports including on its activity and financial management. Fines are envisaged both for the foundations as a legal person and also its responsible person. Fines are presented in Slovenian tolar[30] and amount between 50 000 and 4 million. Sanction in Slovenian tolar can be imposed pursuant to the first and fourth paragraphs of Art. 13 of the Euro Introduction Act (ZUE). The amounts of fines for both types of NPOs do not appear to be effective, or dissuasive. No information is provided on Humanitarian organisations.

Criterion 8.5

(a) The Council of the Government of the Republic of Slovenia for the Promotion of the Development of Volunteering and Volunteer and Non-Governmental Organisations (further Council) is an expert and consultative body of the Government of the Republic of Slovenia. It is composed of 16 members – eight representatives from ministries and government offices, four representatives from NGOs and four representatives from volunteer organisations. Its function consists of monitoring the strategy, the action programme and the development of non-governmental organisations (NGO Act, Art.27).

30. In 2007 the exchange rate was €1 = SIT 239.640.

In addition, the Inspection Act (Art. 11 and 32) establishes the legal basis for cooperation and information exchange between all supervisory authorities. An Inspection Council is established as a permanent inter-ministerial body responsible among others for coordination of the joint performance of inspection tasks of different inspection authorities, addressing common issues.

In Slovenia there are no other established co-operation and coordination mechanisms specifically dealing with the NPOs activities, but in general terms, competent authorities are not prevented from cooperating with each other and exchanging information, including with the LEAs and the OMLP.

(b) The authorities have not indicated relevant specific information about investigative expertise and capability to examine those NPOs suspected of either being exploited by, or actively supporting, terrorist activity or terrorist organisations. Nevertheless, Slovenia clarified that investigative powers are with the Police. In the field of counter-terrorism there is a specific working group led by the Security Agency, where besides the Police and the Security Agency also the OMLP as FIU, FARS, Ministry of Defence, Ministry of Foreign Affairs and Government Office for Migrant Care and Integration are participating.

(c) Authorities indicate that financial and programmatic information can be followed through annual reports, while further access can be granted within the scope of inspection procedures and criminal procedure.

(d) OMLP is responsible for the dissemination of the results of its analyses on suspicion of TF to competent authorities (APMLTF-2, Art. 94). All public authorities and organisations with public powers shall be obliged to report offences for which the perpetrator is being prosecuted ex officio, if they are informed of them or if they otherwise become aware of them (CPA, Art. 145). Tax Procedure Act also provides the framework for sharing information to competent authorities – on request or spontaneously (Art. 23, 24 and 26).

Criterion 8.6

There are no points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support designated in Slovenia. However, those requests are handled within the framework of general international cooperation mechanisms, including MLA, direct cooperation (through Criminal Police Department and SOVA) and FIU-to-FIU cooperation (through OMLP) in place which can effectively employed also for the NPO-specific requests.

Weighting and Conclusion

Slovenia is not properly taking a risk-based approach to NPOs, but the 2025 NRA identified a number of vulnerabilities that are pertinent to all NPOs in general. Slovenia applies multiple mechanisms to promote accountability, integrity and public confidence in the administration and management of NPOs. It undertakes educational programs and training initiative for promoting transparency, integrity, and accountability of NGOs. There is a framework set for encouraging channelling the financial flows through regulated financial institutions. Nevertheless, Slovenia did not demonstrate focused, proportionate and risk-based oversight or monitoring of NPOs. **R.8 is rates PC**.

Recommendation 9 – Financial institution secrecy laws

Slovenia was rated LC with R.9 in the 5th Round MER. The recommendation has not been amended since then. The applicable law has changed but the changes are not considered to be sufficiently material as to warrant a fresh analysis.

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.

Banks are allowed to exchange information where this is necessary for the conduct of negotiations for the conclusion of a contract or for the performance of a contract concluded by the bank in the ordinary course of banking activities (BA, Art. 146(5)). This is equally the case for PSPs and EMIs (PSSIEMPSA, Art. 240(5)). These exemptions could suffice within the context of R. 13 and R.16 but (a) they do not cover R. 17 and (b) they do not cover the whole spectrum of FIs.

Weighting and Conclusion

Financial institution secrecy laws do not generally inhibit the implementation of AML/CFT measures. However, the absence of explicit exemptions from confidentiality provisions related to the exchange of information between all FIs where this is required under R.13, R.16 and R.17 affects the overall rating. **R.9 is rated LC**.

Recommendation 10 – Customer due diligence

In its 2017 MER, Slovenia was rated LC on R.10 due to deficiencies including: no CDD requirements for transactions over EUR 1 000; gaps in the beneficial ownership (BO) definition; no requirement to use reliable sources for BO identification; lack of consideration of life insurance beneficiaries as a risk factor for EDD; broad allowances for delayed verification of customers and BOs; no requirement for FIs to adopt risk management procedures; no explicit CDD requirements for existing customers; and no provision to forego CDD when ML/TF is suspected. R.10 did not undergo a follow-up review.

Since then, Slovenia undertook multiple revisions of the APMLTF. These changes are considered material. On this basis, R.10 is regarded as a RUR.

Criterion 10.1

FIs, are prohibited from opening, issuing or keeping anonymous accounts, password-protected passbook accounts or bearer passport accounts, anonymous safe deposit boxes or other products on behalf of customers enabling, directly or indirectly the concealment of the customer's identity (APMLTF-2, Art. 71). While no reference is made to accounts in obviously fictitious names, the latter part of Art. 71 is sufficiently wide to encompass also this particular form of anonymity.

Criterion 10.2

FIs, have to carry out CDD when:

(a) establishing a business relationship (APMLTF-2, Art. 22(1) Point 1);

(b) carrying out a transaction amounting to EUR 15,000 or more, be it carried out in a single operation or in several operations that appear to be linked (APMLTF-2, Art. 22(1) Point 2;

(c) carrying out occasional transaction involving the transfer of funds in excess of EUR 1 000 (APMLTF-2, Art 23(1)). This threshold does not cover the transfers equivalent to EUR 1 000.

(d) there are grounds to suspect ML/TF in respect of a transaction, customer, assets or property, irrespective of the transaction amount (APMLTF-2, Art. 22(1) Point 5). While a threshold for the carrying out of CDD is to be ignored, the same cannot be said for any exemptions allowed from the carrying out of CDD.

Authorities have advised that to-date the only exemption granted relates to e-money instruments and that CDD shall be carried out if there is a suspicion of ML/TF (APMLTF-2, Art. 27(5)).; and

(e) whenever a FI has doubts about the veracity and adequacy of previously obtained data about a customer or beneficial owner (APMLTF-2, Art. 22(1)(4)).

Criterion 10.3

FIs shall establish the customer's identity and verify the customer's identity on the basis of authentic, independent and objective sources (APMLTF-2, Art. 21(1)). CDD measures are applicable with regards to both individuals and legal persons (APMLTF-2, Arts. 29-30, Art. 36-37). CDD measures are to be carried out also in the case of individual transactions, independently of whether there is a business relationship established or otherwise (see c.10.2).

Criterion 10.4

FIs shall verify the authority under which any person would be purporting to act on behalf of a customer, as well as establish his identity and verify the same (APMLTF-2, Art. 21(2)).

Criterion 10.5

FIs, shall determine who the BO of the customer is (APMLTF-2, Art. 21(1) Point 2). The definition of the BO is largely in line with the standard (see c.24.6 and c.25.4). FIs shall identify a customer's BO as part of their CDD (APMLTF-2, Art. 41(1)). FIs shall verify the identity of any individual determined to be BO (APMLTF-2, Art. 47(2)), which is to be met based on inspecting either the original or copies of business, court or other public register (APMLTF-2, Art. 47(6)). Should this not be sufficient, FIs are to rely on documents provided by the customer (APMLTF-2, Art. 47(7)). FIs are also allowed is to consult the RBO and obtain additional information from other sources to corroborate the information present in the said register (APMLTF-2, Art. 47(6)).

APMLTF-2 provides two key exceptions: one for state or public entities and another for companies listed on regulated markets with disclosure requirements ensuring ownership transparency in line with EU or equivalent international standards. While the former is understandable as the BO vests in society at large and therefore there is a low risk of BO abuse, the latter may present a limitation as it is dependent on there being a sufficient level of transparency due to the applicable disclosure requirements. It is unclear whether 'suitable transparency of ownership' would actually translate into the disclosure of BO. However, the circumstances in which this exemption can find application is quite limited.

The shortcomings noted under c.10.10 are a limitation on meeting the requirements under this criterion.

Criterion 10.6

FIs shall understand the business relationship and obtain data on the purpose and intended nature of the business relationship or transaction (APMLTF-2, Art 21(1) Point 3, Art 53(1)).

Criterion 10.7

FIs shall monitor on a regular basis the business activities of the customer (APMLTF-2, Art. 21(1), Point 4). This general obligation consists of:

(a) an obligation to: (i) verify that a customer's business operations are in line the purpose and intended nature of the business relationship; and (ii) monitor and verify that the customer's business operations are in line with the customer's regular scope of business (APMLTF-2, Art. 54). This has to be done throughout the course of the business relationship, with the scope and frequency thereof to be dictated by the risk presented by the particular business relationship.

(b) an obligation to verify and updating the documents and data obtained on the customer. This is limited to data and documents relevant to customer identification and, where applicable, BO. It does not extend to data or documents collected to establish the purpose or intended nature of the business relationship (APMLTF-2, Art. 54(3) and (4)). The scope and frequency of reviews should be determined by identified risks at both the national and entity level. At a minimum, reviews must occur when there are significant changes in the customer's circumstances, when a FI is legally required to contact the customer to establish BO, and at least every five years after expiry of CDD if the customer has conducted a transaction with the FI in the past twelve months (APMLTF-2, Art. 54(6)).

Criterion 10.8

FIs are required to understand the customer's ownership and control structure (APMLTF-2, Art. 47) and obtain data on the nature of the business relationship (APMLTF-2, Art. 150(1) Point 4). While there is no express requirement for FIs to understand the nature of the customer's business, the on-going monitoring obligations imply that FIs have to understand their customers' business activities (APMLTF-2, Arts. 54(1) and 55(1)).

Criterion 10.9

FIs shall identify the customer and verify its identity through the following information (APMLTF-2, Art. 150(1)):

(a) Name and proof of existence (registration number and tax identification number) - no direct requirement is set to obtain information on the legal form but the legal form can be inferred from the name of the entity itself (Companies Act Art. 19(2)).

(b) Information on the powers that regulate and bind the legal person - no direct requirement is set to obtain this information. The names of the relevant persons having a senior management position in the legal person will be gathered if those act as a legal representative of the legal entity establishing a business relationship or carrying out a transaction.

(c) The address of the registered office.

The authorities have indicated that the remaining information referred to under this criterion may be obtained from documents collected for verification purposes. However, there would still be no obligation on the part of FIs to collect any of the information should it not result from the documents collected for verification purposes.

No express reference is made to legal arrangements and what corresponding data needs to be collected thereon as legal arrangements cannot be established under Slovenian law. However, Authorities have confirmed that provisions for legal persons also apply to legal arrangements, requiring FIs to collect the relevant data.

Criterion 10.10

The criteria for the determination of BO of a legal person are largely aligned with those set by the FATF Standards:

(a) The BO of legal person is defined as being any natural person who directly or indirectly owns a sufficient amount of equity, shares, or voting or other rights so as to allow him or her to participate in the management of the business; or who has a sufficient direct or indirect participating interest in a business entity; or has a controlling position in the management of the business entity. The threshold to determine whether one has the necessary holding to qualify as a BO is set at more than 25% of equity interest, voting or other rights or ownership of 25% plus one of the shares. (APMLTF-2, Art. 42)

(b) Beneficial ownership on the basis of control via other means is considered to arise where a natural person indirectly provides funds to an economic operator and as a result has the power to control directly, or otherwise significantly influence, the decisions of the economic operator's management when deciding on financing and operations, would equally be considered as a BO (APMLTF-2, Art 42(1)-2). This is further elaborated upon to include situations that can result in the consolidation of accounts (APMLTF-2, Art 42(4)). It remains questionable whether the application of controls through other means is sufficient to also capture other informal forms of control such as control exercised through close personal connections to relatives or associates.

(c) The senior managing officials shall be identified as the legal person's BO if: (i) all possible measures have been taken to identify a BO and provided that there are no grounds for suspecting ML/TF (APMLTF-2, Art. 42(5)); (ii) there are any doubts as to who is the BO (APMLTF-2, Art. 42(6)). The representative shall be identified as the legal person's BO if no one is being otherwise identified as a BO. If no beneficial owner can be identified based on control for legal persons where BO cannot be determined through voting rights, shares, or participation interests, the representative shall be designated as the legal person's BO (APMLTF-2, Art. 43(1)). This would also be the case of institutions where the trustee would be considered one of the default BOs (APMLTF-2, Art. 43(3)).

Criterion 10.11

Legal arrangements are not part of Slovenian legal framework and can't be established in Slovenia. Therefore, the requirements for FIs are set only for foreign legal arrangements (APMLTF-2, Art. 21(1), 41(1), and 44).

For customers that are foreign legal arrangements, the FIs shall identify and take reasonable measures to verify the identity of BOs through the following information:

(a) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust (including through a chain of control/ownership).

(b) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

Criterion 10.12

The additional CDD measures to be applied with regards to life insurance and other investment related insurance policies are the following:

(a) where the beneficiary is known - a FI has to obtain the person's full name and, where applicable, the date of birth;

(b) where the beneficiary is defined by characteristics, categories or otherwise - obtain sufficient information and data to ensure that their identity can be established and verified at the time of payment; and

(c) for both the above cases - establish and verify the identity of the beneficiary at the time of the payment (APMLTF-2, Art. 24(3)).

Criterion 10.13

The APMLTF-2 does not contain any provision to consider the beneficiary as a risk factor. However, guidance issued by the ISA state that in assessing the customer risk, FIs are also to take into consideration the beneficiary of a policy (para 4.1.1). However, while a higher risk will trigger an obligation to apply EDD measures, there is no obligation to identify and verify the identity of a beneficiary's BO, where this may be applicable.

Criterion 10.14

FIs shall verify the identity of the customer and BO before establishing a business relationship or conducting transactions for occasional customers (APMLTF-2, Art. 24(1) and Art. 25). Exceptionally, when concerns establishing a business relationship, FIs are allowed to verify the identity of the customer and BO during this process subject to the following conditions: measures to be implemented as soon as possible after the first contact with the customer, its authorised person or statutory representative and there is little risk of ML or TF (APMLTF-2, Art. 24(2)). The APMLTF-2 does not envisage that CDD measures can be applied after the establishment of the business relationship.

Criterion 10.15 – (Not Applicable)

This criterion is not applicable as FIs are required to carry out verification before, or while, establishing any relationship, or before executing a transaction.

Criterion 10.16

Authorities advised that if the legislative change introduces new requirements, OEs shall obtain new data within the time limit prescribed in the transitory provisions of the legislative act. But no evidence was provided to support the statement. FIs are required to revise from time to time the records concerning an OE within a maximum of five-year interval on a risk-sensitive basis (see c.10.7).

Criterion 10.17

FIs shall perform EDD where the ML/TF risks are higher (APMLTF-2, Section 3.3.4.2)

Criterion 10.18

FIs are permitted to apply SDD measures where lower risks have been identified by the country and/or by the FI (APMLTF-2, Art. 62(1-3)). FIs are prohibited from applying SDD measures where there are grounds for suspecting ML/TF (APMLTF-2, Art. 62(5)). There is no outright prohibition against applying SDD measures whenever specific higher risk scenarios apply.

Criterion 10.19

Where FIs cannot meet one or more of the CDD obligations:

(a) they should not establish a business relationship or effect a transaction or shall terminate the business relationship if it already exists (APMLTF-2, Art. 26).

(b) they should consider reporting data on the customer or suspicious transaction to the OMLP.

Criterion 10.20

There is no provision in the law that allows FIs not to pursue CDD requirements where they suspect ML or TF and reasonably believe that performing the CDD process will tip off the customer.

Weighting and Conclusion

There are some criteria that are not met in their entirety. The trigger for CDD under c.10.2(c) is not entirely reflected in the APMLTF-2; information and data obtained to establish the purpose and nature of a business relationship does not seem to have to be reviewed and updated as required in terms of c.10.7; the definition of beneficial owner under c.10.10 is not entirely aligned with the standard; c.10.13 is partly met; there is no restriction as envisaged under c.10.18 with regards to the application of SDD in higher risk scenarios; there are also limitations under c.10.20. **R.10 is rated LC**.

Recommendation 11 – Record-keeping

In its 2017 MER, Slovenia was rated C with R.11. It did not undergo a follow-up review.

Since then, Slovenia undertook multiple revisions of the APMLTF-2 but those did not impact the regulatory framework on record keeping requirements. The changes are not considered material in the context of R.11 and thus, the below analysis represents a summary of 2017 MER findings.

Criterion 11.1

FIs shall maintain data, information and documents collected for CDD purposes (including transaction records) for ten (10) years following the termination of a business relationship or the completion of a transaction (APMLTF-2, Art. 142(1)). Some other longer period may be applicable under one or more other laws. For linked transactions, completion occurs once all operations are carried out, and the retention period begins at that point. The definition of term "transaction" is wide to encompass both, domestic and international transactions. (APMLTF-2, Art. 3(49)).

Criterion 11.2

FIs shall keep all records obtained through CDD measures, account files and business correspondence and results of any analysis undertaken, for at least ten years following the termination of the business relationship or after the date of the occasional transaction (APMLTF-2, Art. 142(1-2)). (see also c.11.1)

Criterion 11.3

FIs shall keep a wide list of different data elements on transaction records. These should be sufficient to allow for the reconstruction of any transaction and provide, if necessary, evidence for prosecution of criminal activity. (APMLTF-2, Art.150(1), Points 6 to 9)

Criterion 11.4

FIs shall ensure that all CDD information and transaction records are available swiftly to domestic competent authorities upon appropriate authority (APMLTF-2, Arts. 99, 126 and 154, CPA, Art. 156).

Weighting and Conclusion

R.11 is rated C.

Recommendation 12 – Politically exposed persons

In its 2017 MER, Slovenia was rated PC with R.12, based on the following deficiencies: an absence of a requirement to take reasonable measures to ascertain the sources of wealth and funds of the BO identified as a PEP; and a lack of clarity on whether the requirement to obtain senior management approval also applies to a BO who becomes a PEP.

In its 2021 FUR, Slovenia addressed all identified deficiencies and R.12 was re-rated as C.

Since then, Slovenia undertook multiple revisions of the APMLTF. These changes are considered material. On this basis, R.12 is regarded as a RUR.

Criterion 12.1

The definition of foreign PEPs generally covers the elements required by the FATF Standards (APMLTF-2, Art. 66(2-3)).

FIs shall take the following measures with respect to foreign PEPs:

(a) put in place risk management systems to determine whether a customer or the beneficial owner is a PEP

(APMLTF-2, Art. 66(1));

(b) obtain senior management approval before establishing and continuing (for existing customers) such business relationships (APMLTF-2, Art. 66(7) Point 2);

(c) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs (APMLTF-2, Art. 66(7) Point 1); and

(d) conduct enhanced ongoing monitoring on that relationship (APMLTF-2, Art. 66(7) Point 3).

When the PEP referred to in this Article ceases to act in a visible public position, the OE shall continue to implement appropriate measures for another 12 months. After this period, it shall assess the subsequent risk posed by that person and take appropriate risk-based measures until it determines that the person no longer poses a risk. This approach is in line with the FATF Guidance on PEPs.

Criterion 12.2

The definition of a PEP covers also domestic PEPs and extends to 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 (APMLTF-2, Art. 66(3), Art. 67). In this regard:

(a) FIs have to have risk management systems to determine whether a customer is a beneficial owner is a PEP (APMLTF-2, Art. 66(1)).

(b) Domestic PEPs and persons entrusted with a prominent function in an international organisation are subject to the same CDD measures as foreign PEPs.

Criterion 12.3

The definition of PEP extends to include immediate family members and individuals with a close relationship with the PEP (APMLTF-2, Art. 66(2, 6-7)).

Criterion 12.4

FIs are required to have adequate measures to establish whether beneficiaries of life insurance and other investment-related insurance policies or their BOs are PEPs. These measures are to be implemented not later than 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 identified, FIs are to take additional measures which include informing 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. 68 of APMLTF-2).

Weighting and Conclusion

R.12 is rated C.

Recommendation 13 – Correspondent banking

In its 2017 MER, Slovenia was rated PC with R.13 due to the following deficiencies: additional measures for FIs applied only to cross-border correspondent relationships with credit institutions from non-EU countries; no explicit requirement for FIs to understand the respondent's business, responsibilities, or assess their AML/CFT controls; requirements to determine the respondent's reputation or supervision quality were insufficient in scope; no specific requirements for payable-through accounts; and no explicit requirement for FIs to be subject to "effective" supervision to avoid being considered a shell bank.

In its 2021 FUR, Slovenia addressed most of the identified deficiencies and R.13 was re-rated as LC.

Since then, Slovenia undertook multiple revisions of the APMLTF. These changes are considered material. On this basis, R.13 is regarded as a RUR.

Criterion 13.1

FIs shall apply enhanced CDD measures when entering into a correspondent banking relationship with a credit institution of FI with its registered office in a Member State or a third country (APMLTF-2, Art. 65). These include the following:

(a) FIs shall understand the nature of the respondent's business and verify customer's reputation and the quality of the supervision it is subject to (APMLTF-2, Art. 65(1)). FIs shall obtain data, information and documents by inspecting public or other accessible data records, or by inspecting documents and business records submitted by the credit or financial institution. (APMLTF-2, Art. 65(1), (3)). However, no reference for FIs to gather information on whether the respondent has been or is subject to ML/TF investigations or regulatory actions.

(b) FIs shall assess the respondent institution's AML/CFT controls (APMLTF-2, Art. 65(1) Point 2).

(c) FIs shall ensure obtaining senior management approval before establishing new correspondent relationships. Absent written approval from senior management, the relationship cannot be entertained. (APMLTF-2, Art. 65(2) and (5) point 2)

(d) FIs have to obtain information about the AML/CFT obligations applicable in the jurisdiction of the respondent institution so that there may be an understanding of each other's AML/CFT obligations (APMLTF-2, Art. 65(1) point 3).

Criterion 13.2

FIs are prohibited from entering into a business relationship or continuing an existing relationship where payable-through accounts are provided where the respondent institution: (a) failed to implement CDD measures on any such third party and; (b) at the request of the correspondent bank, cannot provide the required CDD data, information and documents (APMLTF-2, Art 65(5) point 5).

Criterion 13.3

FIs are prohibited from entering into a business relationship or continue an existing relationship with a credit or a financial institution having its registered office in an EU Member State or a third country and which either operates as a shell bank or otherwise enters into correspondent or other business relationships and conducts transactions with shell banks (APMLTF-2, Art 65(5) point 4).

Weighting and Conclusion

Slovenia implemented requirements for correspondent banking, but some minor shortcomings remain. There is no obligation to consider whether a respondent institution was ever the subject of investigations or regulatory actions **R.13 is rated LC**.

Recommendation 14 – Money or value transfer services

In the 2017 MER, Slovenia was rated as C with R.14. It did not undergo a follow-up review.
Since then, Slovenia undertook multiple revisions of the APMLTF and replaced the Payment Services and Systems Act with the Payment Services, Services of Issuing Electronic Money and Payment Systems Act (PSSIEMPSA). The changes are not considered material in the context of R.14 and thus, the below analysis represents a summary of 2017 MER findings.

Criterion 14.1

Banks, electronic money undertakings and PIs are to undertake payment services based on the authorisation they receive from the BoS (PSSIEMPSA, Art. 34). The Act also provides for waived payment institutions to perform limited money remittances. The BoS can waive some of the authorisation requirements related to the legal form of organisation or the governance and internal control systems for waived institutions (PSSIEMPSA, Art. 76). While EU legislation allows EU-based PIs to operate in Slovenia on the basis of freedom of establishment or freedom to provide services, and without the need of acquiring a separate license, the BoS must be notified by the home country supervisor.

Criterion 14.2

The BoS shall verify whether a natural or legal person is providing payment services without authorisation by examining relevant business books and other documents (PSSIEMPSA, Art. 264). If the conduct of unauthorised payment services is confirmed, BoS can issue a cease-and-desist order or issue a fine ranging from EUR 12 500 to EUR 125 000 EUR (PSSIEMPSA, Art. 310). It may also request the court to initiate the liquidation proceedings when the cease-and-desist order is not complied with (PSSIEMPSA, Art. 267).

Criterion 14.3

MVTS are included in the definition of payment services, which are only allowed to be provided by Payment Service Providers (PSPs) (PSSIEMPSA, Art. 5 and 20). PSPs are designated as obliged entities and are subject to AML/CFT supervision by OMLP and BoS (APMLTF-2, Art. 4(1) and 164(1)). This includes PSPs from other EU Member States that do not need a license in Slovenia, have a branch in Slovenia and are being supervised by BoS in cooperation with the home country supervisor.

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 maintained by BoS (PSSIEMPSA, Art. 79). 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 (PSSIEMPSA, Art. 83).

Criterion 14.5

PSPs are fully responsible for the compliance of their agents with applicable legal requirements (PSSIEMPSA, Art. 46). Thus, PSPs are required to also apply appropriate AML/CFT controls as provided by APMLTF-2 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 (PSSIEMPSA, Art. 43).

Weighting and Conclusion

R.14 is rated C.

Recommendation 15 – New technologies

In its 2017 MER, Slovenia was rated C with R.15. Since then, R.15 has been amended significantly to include new requirements relating to virtual assets (VAs) and virtual asset service providers (VASPs).

In its 2021 and 2022 FURs, Slovenia demonstrated partly addressing the new requirements. In its 2023 FUR, Slovenia addressed most of the identified deficiencies and R.15 was re-rated as LC.

Since then, Slovenia updated its NRA that includes risk assessment on new technologies, VAs and VASPs; undertook multiple revisions of the APMLTF-2; and introduced amendments into other regulatory provisions. Several regulatory developments also took place at the EU level, affecting the compliance of member states with R.15. These changes are considered material. On this basis, R.15 is regarded as a RUR.

Criterion 15.1

At the country-level, the 2025 NRA refers to a number of new or developing technologies for both new and pre-existing products. In particular, it refers to new payment methods like instant payments when it comes to the banking sector and to virtual IBANs and distribution networks when it comes to electronic money. The NRA could benefit from a more thorough assessment thereof. The Action Plan included with the NRA does also seek to strengthen authorities' understanding of these threats through the collection of more reliable data e.g. on virtual IBANs.

FIs shall analyse the impact of all major changes in business processes, including the introduction of new products, new business practices and technologies, as well as changes to their organisation on their ML/TF risk exposure (APMLTF-2, Art. 18(9)). This would therefore include the consideration of how these changes would impact existing products and that the absence of an explicit reference to "delivery mechanisms" would still be covered by changes to the OE's overall practices and processes. This requirement though falls short of covering the risk assessment of developing technologies, the latter being only expressly required for retail banks.

Criterion 15.2

OEs are required to:

(a) The requirement to carry out risk assessment prior to launching or using new products, practices and technologies (APMLTF-2, Art. 18(10)).

(b) OEs shall establish effective policies, controls and procedures to effectively mitigate and manage identified risks of ML/TF (APMLTF-2, Art. 20).

Criterion 15.3

(a) At EU level, the EC conducts and publishes an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities in line with the requirements of the EU Directive 2015/849 as amended by EU Directive 2018/843 (Art. 6) that also identifies and assesses the risks emerging from virtual assets and the activities and operations from VASPs. The EU level risk assessment shall be updated by a report at least every two years.

In line with Art. 7 of EU Directive 2015/849, the results of the above-mentioned supranational risk assessment should also be taken into account at the national level. It is not clear to what extent the country did so when it carried out its 2021 NRA.

The 2025 NRA has sections on both VAs and VASPs. The assessment is based on local data including (i) in the case of VAs the trends in investigations involving VAs and the requests for analysis of crypto-related transactions; and (ii) in the case of VASPs information obtained through supervisors, including the outcome of supervisory examinations, reporting volumes to the OMLP and the nature of the services carried out by VASPs active and registered in Slovenia in the period of 2022–2023. The 2025 NRA contains no reference e.g., to STRs or requests for information from foreign counterparts involving VAs or VASPs. It is therefore difficult to say whether (i) the Medium-High ML/TF/PF threat level in the case of VAs; and (ii) the High ML/TF residual risk level in the case of VASPs reflects the actual risk or otherwise.

(b) Based on its understanding of risks:

(i) Slovenia is expected to take risk-based measures to mitigate the ML/TF risks in the sector (APMLTF-2, Art. 14(2)).

(ii) Slovenia is expected to implement risk-based measures commensurate with the risks identified and allocate resources in line with (APMLTF-2, Art. 14 (2) point 3)

The 2025 NRA sets out an Action Plan which includes an action point specifically on VASPs related to the need to ensure greater attention to the carrying out of unauthorised activities. The analysis on VASPs in the NRA suffered from some limitations in terms of the granularity of the data available on their operations as well as highlighted issues in relation to their proper implementation of AML/CFT mitigating measures and reporting to the OMLP. No action items on these aspects have been included, reliance instead being made on the coming into force of MiCAR as a possible solution. However, MiCAR will not of itself result in proper implementation of AML/CFT obligations nor in increased reporting.

With regards to the use of virtual assets, no specific action point has been included though there are more general ones like increasing the quality and quantity of resources available to LEAs which could be considered as also including a reference to increased resources available to tackle crypto-related crime.

It is difficult to say whether these measures are adequate and proportionate to the ML/TF/PF risks faced by Slovenia through the use and abuse of virtual assets and VASPs as the risk assessment itself suffers from a lack of sufficient data to allow a proper analysis in this regard.

(c) The APMLTF-2 refers to Regulation (EU) 2023/1114 when defines 'crypto-asset' and 'crypto-asset services' Given that these definitions in Regulation (EU) 2023/1114 are aligned with the FATF standard, it follows that Slovenia is aligned with the FATF Standards as well.

Insofar as the risk mitigation measures that covered VASPs have to apply in relation to any identified ML/TF/PF risks, reference is made to c.1.12, c.1.13, c.1.14 and c.1.15.

Criterion 15.4

(a) A person providing crypto[31] asset services within the EU is subject to prior authorisation (EU Regulation 1114/2023, Art. 59) by the authority of the member state where it has its registered office. A crypto asset service provider under EU law should be a legal person or other undertaking if the legal form of that undertaking ensures a level of protection for third parties' interests equivalent to that afforded by legal persons and if it is subject to equivalent prudential supervision appropriate to their legal form (Art. 59 (3)). These requirements to the legal form of undertakings exclude natural persons from being authorized as crypto asset service providers (c.15.4(a)(ii) is not applicable).

EU law also subjects some types of offerors to authorisation requirements and differentiates offerors according to the specific assets: A person that issues virtual assets qualifying as asset-referenced tokens (EU terminology for a type of stable-coins) has to be authorized as well (EU Regulation 2023/1114, Art. 16). E-money tokens may only be issued by authorized credit institutions or e-money institutions (EU Regulation 2023/1114, Art. 48). Financial services related to an issuer's offer and/or sale of a virtual asset are covered in the crypto-assets services list under Art. 3 (1)(16) of EU Regulation 2023/1114, in line with the provisions of the FATF glossary and the Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers[32] for limb (v) of the VASP definition in the FATF glossary.

31. In the terminology of the EU Regulation 1114/2023 on markets in crypto-assets 'virtual asset' and 'virtual asset service provider' as per the FATF Glossary are defined as 'crypto asset' and 'crypto asset service providers' respectively. Here, both terms are used depending on the framework referred to.

32.https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf

Authorisation processes for service providers and offerors include a fit and proper assessment and authorisations shall only be granted if members of the management bodies and shareholders or members are of sufficiently good repute (Art. 21 (2), 63 (10) of EU Regulation 2023/1114).

Slovenia has identified the SMA as the national authority responsible to authorise crypto-asset service providers under EU Regulation 2023/1114. Any legal person having its registered office in Slovenia cannot provide crypto-asset services unless authorised by the SMA in line with Art. 62(1) of EU Regulation 2023/1114. Legal persons that have their registered office in another EU Member State can offer products and/or services to customers in Slovenia on the basis of the passporting rights under Art. 65 of EU Regulation 2023/1114. This would be dependent on the competent authority within the home Member State notifying beforehand the SMA. The requirement to have a registered office within an EU Member State excludes the possibility of anyone established outside the EU providing services within an EU Member State.

Offerors are equally subject to oversight by the SMA for the purposes of the said regulation, with the exception of offerors of e-money tokens which fall under the purview of the BoS (Implementation of Regulation (EU) on Markets in Crypto-Assets Act, Art. 3).

In cases of banks, the authorisation to also provide crypto-asset services is subject to approval by the BoS (BA, Art. 31). Whenever this is done, the BA has to inform the SMA.

(b) The authorisation processes under EU Regulation 2023/1114 include assessments that members of the management body are sufficiently reputable and competent and that shareholders or members that have a qualifying holding fulfil fit and proper requirements (MiCAR, Arts. 62, 63, 64 and 68 for crypto asset service providers). These provisions empower authorities to prevent individuals convicted of offences relating to ML or TF or of any other offences that affect their good repute from assuming relevant functions. Regarding shareholders and members whether direct or indirect, that have qualifying holdings, proof is required that those persons are of sufficiently good repute (MiCAR, Art. 62(2)(h)).

While particular emphasis is made on criminal investigations and convictions, guidelines issued by the EBA and ESMA also highlight the need to take into account other information from reliable and credible sources that show that the individual may not of sufficiently good repute. Taking into account that MiCAR allows national competent authorities to consult with AML/CFT supervisors and with FIUs (Art. 83(5)) as may be deemed necessary, it follows that there are the necessary powers and discretion to also allow for the detection of criminal associates.

Any member of the management body, shareholder or member having a qualifying shareholding has to continue meeting the requirements referred to above on an on-going basis (MiCAR, Art. 64(1)(e)), as not doing so may be grounds for the withdrawal of the authorisation so granted. The SMA can demand the removal/replacement of a member of the management body that is no longer deemed to be fit and proper (MiCAR, Art. 94(1)(y)) but there does not seem to be the possibility to require a qualifying shareholder that is no longer deemed of sufficiently good repute to divest itself of its holding. Art. 68(3) of MiCAR requires competent authorities to be able to take steps where the qualified shareholder is negatively impacting the prudent management of the authorised entity. It then provides examples of what these measures may be, but it is does not seem that the SMA has been empowered to exercise any of these or similar ones. Changes within the management body and within the shareholders or members holding a qualifying shareholding shall be notified to the national competent authority, i.e. the SMA. In the case of members of the management body, any such notification has to take place prior to any such individual exercising its functions (MiCAR, Art. 69). However, it is unclear whether any such change can take effect once the notification requirement has been met or whether it is dependent on the SMA granting its approval thereto. With regards to changes in members or shareholders holding a qualifying shareholding, there is a prior notification requirement under Art. 83 and the change can only take place once the SMA has approved the same.

The SMA has indicated that its requirements are aligned with the above and that it is also seeking information from the OMLP and the BoS on applicants for authorisation, including proposed members of the management body and proposed holders of qualifying shareholdings on the basis of existing legal provisions and MOUs. However, the information provided does not allow for a proper assessment as to whether the SMA's authorisation process meets the sub-criterion's requirements.

Criterion 15.5

Regulation at EU level prohibits the provision of services without authorisation (EU Regulation 2023/1114, Art. 59(1)). EU Regulation 2023/1114 task competent authorities in member states to ensure action is taken to identify persons that carry out VASP activities without licensing or registration and to ensure compliance with authorisation requirements by taking supervisory measures and applying sanctions. EU Regulation 2023/1114, Art. 94(1)(h) stipulates those competent authorities, in accordance with national law, shall have the power to order the immediate cessation of the activity where there is a reason to assume that a person is providing crypto-asset services without authorisation. The prerequisite of "reason to assume" the provision of service leaves sufficient room to take targeted action at service providers that address the market. At EU level, the European Securities and Markets Authority assist efforts to ensure compliance by keeping a register of operators found to have provided services in breach of the authorization requirement (Art. 110 of EU Regulation 2023/1114).

At national level, to abide by the requirements under EU Regulation 2023/1114 the Law on the implementation of Regulation (EU) on Markets in Crypto-Assets does provide for the imposition of administrative penalties in line with Art. 111 of EU Regulation 2023/1113 ranging from a minimum of EUR 2 500 to EUR 500 000 depending on the size of the entity which is determined on the basis of average number of employees, net turnover and value of assets. This may be seen as ensuring a degree of proportionality in the administrative penalties that may be imposed but considering that the maximum penalty would represent only 1% of the turnover of the smallest large companies or 2% of its asset value, it is questionable whether this is the case. In part, this may be addressed through a higher threshold of penalties. Depending on the severity of the breach, the administrative penalty may be increased to a maximum of EUR 5 million or 5% of its annual turnover as results from the latest available financial statements, or twice the gain realised or loss avoided, depending on which is the higher. It is unclear under what circumstances unauthorised activity would be considered as particularly serious as to trigger the application of this latter bracket of penalties. A particularly serious breach is based on the amount of damage caused or the amount of unlawful material gain obtained, or due to the offender's intention or his intention of self-interest but there is no clear policy on how these are criteria are determined and applies, with penalties imposed on a case-by-case basis. Any decision to impose an administrative measure is subject to publication on the SMA's website as per Art. 114 of EU Regulation 2023/1114.

The SMA has clarified that it actively monitors the market by shifting through internet pages and social media. All of this is complemented by information it collects through other means like consumer complaints, or information obtained through ESMA. In line with its Supervisory Procedures, in the event that it detects instances of unauthorised activities it can also issue cease and desist orders.

Cooperation with the BoS is also key due to possible legacy issues. Until the applicability of MiCAR and the transposition of relevant provisions thereof, the BoS was the national authority responsible for supervising the national registration framework for services similar to crypto-asset services. This cooperation will be useful to detect any service provider that following the end of the transitory period will not have migrated to the MiCAR regime to assess whether they have effectively ceased to provide services. Though a process is being ironed out between the two authorities, the AT has been informed that there were already instances where the BoS highlighted possible cases of unauthorised activity to the SMA.

Criterion 15.6

(a) When assessed for market entry, crypto asset service providers shall have mechanisms and controls in place that ensure compliance with AML/CFT requirements (EU Regulation 2023/1114, Art. 63(2) to (10)). When it comes to the actual monitoring and supervision of VASPs with AML/CFT obligation, the function under the APMLTF-2 is vested in OMLP and the SMA (APMLTF-2, Art. 153(1) and Art. 164(1)). The BoS still has responsibility for supervising those banks, PSPs and EMIs that also provide crypto-asset services. The shortcomings in the risk assessment and supervisory methodologies for the BoS and SMA identified under c.26.5 and c.26.6 are equally applicable in this context.

(b) EU Directive 2015/849 and EU Regulation 2023/1114 task competent authorities in member states to ensure compliance by crypto asset service providers with requirements to combat money laundering and terrorist financing. EU Regulation 2023/1114, Art. 94, stipulates that competent authorities in accordance with national law shall have the power to inspect and to compel documents. The withdrawal of the authorisation of crypto asset service providers is regulated at EU level in Art. 64 of EU Regulation 2023/1114 and, alongside other administrative penalties and administrative measures, shall also be implemented at national level (EU Regulation 2023/1114, Art. 111).

At a national level the main responsibility for monitoring compliance with AML/CFT obligations rests with the OMLP and the SMA (APMLTF-2). The assessment carried out under R.27 with regards to the OMLP is equally applicable in this case. With regards to the SMA, the Act on the Implementation of the Markets in Crypto-Assets Regulation provides the SMA with the necessary powers to conduct on-site and off-site inspections as well as to request documents and information for supervisory purposes (Art 6 and Art 7). As already stated, Art. 64 of EU Regulation 2023/1114 does provide for the withdrawal of an authorisation for breaches of AML/CFT obligations.

Criterion 15.7

After amendment by EU Regulation 2023/1113 EU Directive 2015/849 (Art. 18) mandates the European Banking Authority to issue guidelines on risk variables and risk factors to be taken into account by crypto-asset service providers when entering into business relationships or carrying out transactions in crypto-assets. (Guidelines published on 16 January 2024 and to be applied from issued from 30 December 2024).

At the national level, the analysis under R.34 is equally applicable here. The BoS has issued sectoral guidelines applicable to VASPs in 2022 as well as incorporating within its framework the risk-factor guidelines issued by the EBA. However, it has to be remarked that these would at present be applicable only to banks, EMIs, and PSPs that also offer crypto-asset services. The SMA has held meetings with prospective VASPs but has so far not issued any guidance that may be applicable to VASPs. Moreover, no information has been provided on the actual feedback that may be provided by OMLP on the reports submitted by VASPs.

Criterion 15.8

(a) At the EU level, EU Directive 2015/849 and EU Regulation 2023/1114 require member states to provide competent authorities, in accordance with national law, with the power to apply appropriate administrative penalties and other administrative measures. Art. 111 of EU Regulation 2023/1114 stipulates sanctions for a number of infringements including minimum fines.

At the national level, analysis under c.35.1 applies here.

(b) In addition, Member states are obliged to ensure that where obligations apply to legal persons in the event of a breach, sanctions and measures can be applied to the members of the management body and to other natural persons responsible for the breach (Art. 58(3) of EU Directive 2015/849). Some of the administrative penalties regulated under EU Regulation 2023/1114, Art. 111, shall also apply to members of the management body of a crypto-asset service provider.

At the national level, analysis under c.35.2 applies here.

Criterion 15.9

*(*a) All OEs shall conduct CDD of a customer in the event of any occasional transaction involving the transfer of funds in excess of EUR 1 000 (APMLTF-2, Art. 23(1)). However, it is unclear whether the reference to 'funds' also captures crypto-assets.

(b) (i) EU Regulation 2023/1113 repeals and replaces EU Regulation 2015/847 formerly regulating the transfer of funds and extends the scope to cover both transfer of funds and transfer of virtual assets. Art. 14(1) of EU Regulation 2023/1113 requires the originating crypto asset service provider to obtain and hold originator information (Art. 14(1), (2) and (3)) and to submit it to the beneficiary service provider immediately (in advance or simultaneously) and securely (Art. 14(4)). Before transferring crypto-assets, the service provider shall verify the accuracy (Art. 14(6). In accordance with Art. 24 of EU Regulation 2023/1113, information has to be provided to competent authorities in the Member State in which they are established. The originating crypto asset service provider submits beneficiary information to the beneficiary's service provider in line with Art. 14(2) of Regulation 2023/1113 and holds it on record according to Art. 26(1) Regulation 2023/1113.

The distributed ledger address (DLT) information is required for both the originator and the beneficiary. If the transfer does not occur on the DLT, the Regulation requires the crypto-asset account number instead (EU Regulation 2023/1113, Art.14(1)(b) and (2)(b)).

EU Regulation 2023/1113 imposes additional requirements to be implemented in the case of transfers being made to self-hosted addresses (where no crypto asset service provider is involved on the originator or beneficiary side), such as individual identification of transfers and ensuring that the address is controlled by the originator/beneficiary.

EU Regulation 2023/1113 does not make a distinction between crypto-asset transfers within and outside the EU, treating all crypto-asset transfers as cross-border.

(ii) Art. 16 of EU Regulation 2023/1113 requires the crypto asset service provider of the beneficiary to implement effective procedures, which may include post-event or real-time monitoring, to identify transfers that lack required originator or beneficiary information and to verify accuracy of the beneficiary information (EU Regulation 2023/1113, Art. 16(1) and (3)). Service providers are obliged to make information available to competent authorities on request according to Art. 24 of EU Regulation 2023/1113.

(iii) EU Regulation 2023/1113 covers the requirements of Recommendation 16 and applies them to virtual asset transfers, especially on monitoring and risk-based procedures (Art. 14(8) and Art. 16(1)) as well as freezing action and prohibiting transactions with designated persons and entities (Art. 23).

(iv) Financial institutions are covered by the scope of relevant provision of EU Regulation 2023/1113 through the broad definition of crypto asset service provider in Art. 3(1)(15) of that Regulation with reference to Art. 3(1)(15) EU Regulation 2023/1114, including credit institutions that provide crypto asset services in accordance with Arts. 59, 60 of EU Regulation 2023/1114.

Criterion 15.10

The EU regulations imposing TFS pursuant to UNSCRs 1267/1988, 1989 and 1373 (TF TFS) as well as UNSCRs 1718 and 2231 (PF TFS) apply to all natural and legal persons, thus including VASPs (CR 753/2011, Art. 14 - CR 881/2002, Art. 11 - CR 2580/2001, Art. 10 - CR 2017/1509, Art. 1 - CR 267/2012, art.49). Issues related to EU internals persist.

Mechanisms for communicating designations as well as reporting and monitoring obligations described in criteria 6.5(d), 6.5(e), 6.6(g), 7.2(d), 7.2(e), 7.3 and 7.4(d)) also apply to VASPs.

Deficiencies in respective criteria under R.6 and 7 apply here respectively.

Criterion 15.11

EU Regulation 2023/1114, Art. 107, expressly provides that competent authorities should, where necessary, conclude cooperation arrangements with supervisory authorities of third countries concerning the exchange of information with those supervisory authorities of third countries and the enforcement of obligations under this Regulation in those third countries.

This provision complements Art. 95 to Art. 97 of EU Regulation 2023/1114 which provide for cooperation within an EU context both between national authorities as well as between national and supranational authorities. These provisions would be applicable with regards to the SMA and, to a more limited extent, the BoS.

In addition, Slovenia has legal provisions allowing for a broad international assistance for investigations, prosecutions, and proceedings related to ML, FT, and associated offences (see R.37-40). In addition, the OMLP is verted with broad powers for international cooperation when acting as a VASP supervisor (APMLTF-2, Art. 115(1) and Art. 155(1).

Weighting and Conclusion

Slovenia implemented requirements for new technologies, but some moderate shortcomings remain. There are still issues with the quality of risk understanding at the national level, especially when it comes to virtual assets and VASPs (c.15.3). In particular, shortcomings under c.15.4 may lead to associates of criminal elements not being identified when assessing beneficial owners and members of the management body. Concerns also remain as to the adequacy of the guidance and feedback provided (c.15.7), sanctions imposed for breaches of AML/CFT obligations (c.15.8) and with regards to the application of TFS (c.15.10) **R.15 is rated PC**.

Recommendation 16 – Wire transfers

In its 2017 MER, Slovenia was rated PC with R.16, based on the following deficiencies: an absence of requirements in relation to beneficiary information; and a lack of a requirement for intermediary FIs to identify missing originator or beneficiary information and to implement the risk-based policies. In its 2018 FUR, following the adoption of EU Regulation 2015/847, Slovenia addressed all the identified deficiencies and R.16 was re-rated as C.

Since then, the EU Regulation 2015/847 was replaced by EU Regulation 2023/1113. These changes are considered material. On this basis, R.16 is regarded as a RUR.

Criterion 16.1

In accordance with EU Regulation 2023/1113, Arts. 4, 6, FIs should ensure that all cross-border wire transfers exceeding EUR 1 000 are accompanied by:

(a) required and accurate payer (originator) information (name, account number or, in the absence of an account, unique transaction reference, and address, document number, customer ID, or date and place of birth), and

(b) required payee (beneficiary) information (name, account number or, in the absence of an account, unique transaction reference)

The EU requirements for cross-border transfers do not apply to transfers equalling USD/EUR 1 000, which constitutes a minor deviation from the corresponding Recommendation.

Criterion 16.2

Where several cross-border wire transfers from the same originator are transmitted in a batch file to beneficiaries, the batch file should contain the information required per criterion 16.1, and each individual wire transfer should contain the account number or unique reference number (EU Regulation 2023/1113, Arts. 4, 6(1)).

Criterion 16.3

Cross-border wire transfers of EUR 1 000 or less should be accompanied by the names and account numbers of the originator and beneficiary or the unique transaction reference number (EU Regulation 2023/1113, Art. 6(2)).

Criterion 16.4

For cross-border wire transfers not exceeding EUR 1 000, the originator's financial institution is not required to verify the accuracy of the information about the originator unless it suspects ML/TF, or the funds are transferred in the form of cash or anonymous electronic money (EU Regulation 2023/1113, Art. 6(2)). The same applies to the beneficiary’s financial institution (EU Regulation 2023/1113, Art. 7(4)).

Criterion 16.5

For wire transfers with all participants in the payment chain established within the EU, Art. 5(2) of EU Regulation 2023/1113 obliges the service provider of the payer, upon request, to make all information on the originator or beneficiary available to the beneficiary's financial institution. Based on the availability of this information by other means, Art. 5(1) of EU Regulation provides for a derogation of the comprehensive information requirements in line with c.16.5.

Criterion 16.6

FIs should ensure that the account numbers of the originator and beneficiary or their unique transaction identifiers accompany the transfer (EU Regulation 2023/1113, Art. 5(1)) even in applying the derogation in line with c.16.5. FIs are required, upon request, to make all necessary information available within three working days (EU Regulation 2023/1113, Art. 5(2)). They are also required to respond fully and without delay to requests issued by the authorities responsible for AML/CFT (EU Regulation 2023/1113, Art. 24).

Criterion 16.7

The originator's FI shall maintain all information collected on the originator and beneficiaries for a period of five years (EU Regulation 2023/1113, Art. 26).

Criterion 16.8

The originator's FU is not allowed to execute wire transfers if they do not comply with the requirements under criteria 16.1 to 16.7 (EU Regulation 2023/1113, Art. 4(6)).

Criterion 16.9

FIs acting as intermediaries should ensure that all originator and beneficiary information accompanying cross-border wire transfers is retained with the transfer (EU Regulation 2023/1113, Art. 10).

Criterion 16.10 – (N/A)

Technical limitations cannot justify non-compliance with the requirements under Art. 10 of EU Regulation 2023/1113 and no exemption from the requirements described under criterion 16.9 is permitted. The "Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under EU Regulation 2023/1113" issued by the European Banking Authority on 4 July 2024 reflect that systems have to be able to transmit, receive or convert all information (section 4.3.1., paras. 21, 22).

Criterion 16.11

Intermediary FIs should implement effective procedures to identify cross-border wire transfers that lack the required originator or beneficiary information (EU Regulation 2023/1113, Art. 11, point 2(b)).

Criterion 16.12

Intermediary FIs should have risk-based procedures in place to determine whether to execute, reject or suspend a wire transfer that does not include the required originator or beneficiary information, and to take appropriate follow-up action (EU Regulation 2023/1113, Art. 12).

Criterion 16.13

FIs should implement effective procedures, which may include post-event or real-time monitoring, to identify cross-border wire transfers that lack required originator or beneficiary information (EU Regulation 2023/1113, Art. 7(2)).

Criterion 16.14

For wire transfers exceeding EUR 1 000, the beneficiary's financial institution should verify the identity of the beneficiary (EU Regulation 2023/1113, Art. 7(3)) and should retain this information for a period of five years (EU Regulation 2023/1113, Art. 26). For wire transfers equalling EUR 1 000, the beneficiary's financial institution is not required to verify the accuracy of the information unless it suspects ML/TF or the funds are transferred in the form of cash or anonymous electronic money (EU Regulation 2023/1113, Art. 7(4)), which constitutes a minor deviation from the corresponding Recommendation.

Criterion 16.15

Beneficiary financial institutions should have risk-based procedures in place to determine whether to execute, reject or suspend a wire transfer that does not include the required originator or beneficiary information, and to take appropriate follow-up action (EU Regulation 2023/1113, Art. 8).

Criterion 16.16

EU Regulation 2023/1113 applies to PSPs established in the EU or EEA that execute fund transfers, whether they operate directly or through their agents (EU Regulation 2023/1113, Art. 2(1)).

Criterion 16.17

(a) Payee and intermediary PSPs should take into account missing or incomplete information on the originator or beneficiary in order to assess whether a suspicious transaction report should be filed (EU Regulation 2023/1113, Art. 9 and 13).

(b) There is no explicit obligation requiring PSPs to file a STR in all countries concerned by a suspicious wire transfer. However, PSPs are obliged to report in the countries of the ordering and beneficiary sides

(Regulation (EU) 2023/1113, Arts. 9 and 13) of the transaction and service providers belonging to the same financial group shall inform the members of the group of the existence and content of a suspicious transaction report relating to a common client (APMLTF-2, Art. 78(3)).

Criterion 16.18

FIs should implement freezing measures and comply with prohibitions from conducting certain transactions in accordance with EU regulations which give effect to UNSCR relating to AML/CFT (cf. R.6 and 7). EU Regulation 2023/1113, Art. 23 requires PSPs to have in place internal policies, procedures and controls, in alignment with the Guidelines adopted pursuant to Art. 23(2) of the Regulation to ensure the implementation of EU and national restrictive measures.

Weighting and Conclusion

Slovenia implemented requirements for wire transfers, but some minor shortcomings remain. There are still some minor deficiencies present, namely in terms of a slightly higher threshold than what is provided for under c.16.1, c.16.4 and the absence under c.16.17 of an explicit obligation to file a STR in all concerned countries. **R.16 is rated LC.**

Recommendation 17 – Reliance on third parties

In its 2017 MER, Slovenia was rated LC with R.17, based on the following deficiencies: a lack of requirements regarding third parties established in EU Member States; and an absence of specific obligations to adequately mitigate higher country risk at the group level. R.17 did not undergo a follow-up review.

Since then, Slovenia undertook multiple revisions of the APMLTF. The changes are not considered material in the context of R.17 and thus, the below analysis represents a summary of 2017 MER findings.

Criterion 17.1

Reliance is allowed on certain types of FIs to perform CDD measures except for the ongoing monitoring of the business relationship. Ultimate responsibility for the proper application of CDD measures rests with the relying FIs (APMLTF-2, Art. 56 (1)(4)).

(a) and (b) A third party should immediately provide CDD data and documents to the relying institution upon request. (APMLTF-2, Art. 56(1), 59 (1)-(3)). FIs must make sure in advance that third parties can meet these requirements (APMLTF-2, Art. 56(2)). FIs are prohibited from establishing a business relationship with a customer if the third party fails to provide the CDD data in advance (APMLTF-2, Art. 59(5)).

(c) FIs are not required 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. No such requirements apply when reliance is being exercised on a third party located within an EU Member State (APMLTF-2, Art. 57) whereas where reliance is exercised on a third party located in a country other than an EU Member State, the FI does not have an obligation to determine whether the entity relied upon is subject to regulation.

Criterion 17.2

Reliance on third parties that are established in third countries listed as high-risk are prohibited (APMLTF-2, Art. 57(6)). However, the third party reliance is permitted in case of EU Member States without having regard to the level of country risk, which falls short of the c.17.2. FIs are also allowed 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 (APMLTF-2, Art. 57(7))

Criterion 17.3

FIs are allowed to entrust the application of CDD measures to a third party which is a member of their group (APMLTF-2, Art. 60) 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 APMLTF-2 or other regulations;

(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

Slovenia implemented requirements on reliance on third parties, but some minor shortcomings remain. These include: (i) 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; (ii) permitting reliance in case of EU Member States or their branches and majority-owned subsidiaries in third countries without having regard to the level of country risk (iii) there is no specific requirement to adequately mitigate the higher country risk at the group level, which contradicts the c.17.3. Slovenia. **R.17 is rated LC.**

Recommendation 18 – Internal controls and foreign branches and subsidiaries

In its 2017 MER, Slovenia was rated LC with R.18 due to lack of requirements for training on policies, controls, and procedures; deficiencies in group policies; and lack of requirements for third parties in EU Member States. The 2018 FUR showed most issues were addressed, but R.18 remained LC.

Since then, Slovenia undertook multiple revisions of the APMLTF. These changes are considered material. On this basis, R.18 is regarded as a RUR.

Criterion 18.1

FIs shall establish effective policies, controls and procedures that are in proportion to their activity and size (APMLTF-2, Art. 20(1)). The policies, controls and procedures are to effectively mitigate and manage any identified ML/TF risks and, amongst others, are to include:

(a) Compliance management arrangements – FIs shall appoint an "authorised person" (APMLTF-2, Art. 83(1)). Such a person must hold a position that is high enough in rank to enable the rapid, quality and timely execution of tasks (APMLTF-2, Art. 84(1)). This satisfies the requirement of holding a managerial position. FIs, 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 (APMLTF-2, Art. 20 (3)).

(b) Policies, controls and procedures shall also cover secure employment and, if required, security clearance of employees governing classified information. (APMLTF-2, Art. 20 (1) and (2)). Conditions for suitability of AML/CFT compliance officers are defined in Art. 84 APMLTF-2.

(c) Policies, controls and procedures must cover employee training (APMLTF-2, Art. 20(2)). Additionally, reporting entities are to conduct regular training for all employees carrying out tasks for the prevention and detection of money laundering and terrorist financing pursuant to APMLTF-2 (Art. 87).

(d) Policies, controls and procedures shall also cover establishment of an independent internal audit department to verify internal policies, controls and procedures if a FI is a medium-sized or large company as per the Act governing companies (APMLTF-2, Art. 20(2)(2)).

Criterion 18.2

FIs that have branches and majority-owned subsidiaries in Member States or third countries shall establish effective policies, controls and procedures with regard to the risk exposure of the group as a whole and implement those in branches and majority-owned subsidiaries (APMLTF-2, Art. 20(4) and 78(2)). These group-wide programmes must cover the same points as described under c.18.1 (APMLTF-2, Art. 20(2)) as well as the following:

(a) Policies and procedures for intra-group information exchange aimed at preventing money laundering and terrorist financing (APMLTF-2, Art. 78(1-2)). This explicitly includes exchange of information on CDD (APMLTF-2, Art. 78(4) and Art. 150), but does not equally contain an explicit reference to information exchange required for the ML/TF risk management purposes. While this can be implied through the overarching general obligation of information exchange as well as through other obligations as in the context of the obligation to carry out a group-wide risk assessment (APMLTF-2, Art. 18(5)), it cannot be concluded that this is actually the case.

(b) There is no specific requirement on provision of information to or from the group-level compliance, audit and/or AML/CFT functions. Exchange of information only explicitly includes data on customer, accounts and transactions, also STRs unless the OMLP explicitly opposes (APMLTF-2, Art. 78(3-4) and Art. 150). Thus, it cannot be concluded that the requirements of this sub-criterion are met.

(c) No information can be transferred to a third country unless the country meets specific data protection requirements (APMLTF-2, Art. 78(5)). However, no other safeguards on the confidentiality and use of information exchanged is provided for.

Criterion 18.3

FIs have an overall obligation 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 APMLTF-2, where accommodated in the law of the third country (countries outside of EU) (APMLTF-2, Art. 82(1)). 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 APMLTF-2, a FI shall ensure that its branches or its majority-owned subsidiaries adopt and implement suitable measures equivalent to the measures prescribed in APMLTF-2, within the laws of the respective third country (APMLTF-2, Art. 82(2)). 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), a FI 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 (APMLTF-2, Art. 82(4)). The BoS, SMA and ISA are to notify the EBA and competent supervisory bodies of other Member States of this, namely for the purpose of harmonising activities in finding a suitable solution (APMLTF-2, Art. 82(3)). There are no provisions regulating application of AML/CFT measures consistent with home country requirements for FIs that have branches or majority – owned subsidiaries in the EU Member States.

Weighting and Conclusion

Slovenia implemented requirements on reliance on internal controls and foreign branches and subsidiaries, but some minor shortcomings remain. These include issues with: (i) obligation to share information within a group; (ii) safeguards on the confidentiality and use of information; (iii) application of AML/CFT measures consistent with home country requirements for FIs that have branches or majority – owned subsidiaries in the EU Member States. **R.18 is rated LC.**

Recommendation 19 – Higher-risk countries

In its 2017 MER, Slovenia was rated LC with R.19, based on the following deficiencies: a lack of explicit requirement to apply EDD measures proportionate to the risks to business relationships and transactions with natural and legal persons (including FIs) from countries for which this is called for by the FATF; and the limitation of the "special care" provision only to unusual transactions. R.19 did not undergo a follow-up review.

Since then, Slovenia undertook multiple revisions of the APMLTF-2. These changes are considered material. On this basis, R.19 is regarded as a RUR.

Criterion 19.1

FIs shall apply EDD when a customer or a transaction is related to a high-risk third country (APMLTF-2, Art. 64(1(4)) and Art. 69). The list of high-risk countries is the one adopted by the EC (Directive 2015/849) (APMLTF-2, Art. 55(6) and Art. 69(1)). FATF-listed countries are included in an additional list published by the OMLP. In this latter case, EDD measures are to be applied only if the FI considers the overall business relationship or occasional transaction to present a high risk of ML/TF, allowing the FI discretion as to whether to do so or otherwise. This does not satisfy the requirement of applying EDD measures to countries for which this is called for by the FATF which allows the exercise of discretion in so far as the intensity of the EDD measures but not whether they should be applied or otherwise.

Criterion 19.2

When dealing with high-risk jurisdictions independently of any call by the FATF, but on the basis of the EC list, FIs have to apply EDD measures as are listed under Art. 69(1). In addition thereto, supervisory authorities may request the FI to apply additional countermeasures, such as: (i) using additional EDD elements; (ii) introduce enhanced relevant reporting mechanisms or systematic reporting of data to the OMLP; (iii) limit business relationships or transactions (APMLTF-2, Art. 69(1-2)). These countermeasures can be requested by the supervisor where appropriate, which Authorities interpret as requests that have to be risk-based.

Criterion 19.3

The OMLP shall publishing the list of the EC's high-risk countries (APMLTF-2, Art. 55(6)). It shall prepare a list of countries in which there is a higher probability of ML/TF risk, taking into consideration data from competent international organisations (e.g., FATF, OECD, UNODC, etc.) and publish it on its website (APMLTF-2, Art. 55(7)).

Countries on the list are divided into: (i) countries that have a high risk of ML/TF, and (ii) countries with an increased risk of ML/TF. The list is updated on a regular basis, depending on when organisations who publish lists taken into account by the OMLP update their own lists. The OMLP list includes links to the different lists, which include additional information as to the main reasons for a jurisdiction being so listed. The OMLP list is published on, and is publicly accessible through the OMLP website. A newsletter advising that a new revised list has been uploaded is circulated to subscribers thereof.

Weighting and Conclusion

Slovenia implemented requirements relative to higher risk countries, but some minor shortcomings remain when it comes to FATF listed countries. **R.19 is rated LC**.

Recommendation 20 – Reporting of suspicious transaction

Slovenia was rated C with R.20 in the 5th Round MER. Since then, Slovenia amended the applicable law. These changes are considered material. On this basis, R.20 is regarded as a RUR.

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. 76 of the APMLTF-2. 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 associated with money laundering 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 next business day at the latest) or in writing.

However, where suspicion with regards to a transaction only arises following its execution, the FI has to report the same immediately or not later than five business days after having identified the grounds for suspicion or having sufficient information to be able to identify the grounds for such suspicion. This mechanism to file STRs casts doubts on fulfilment of the obligation to do so "promptly" in line with the FATF Recommendations.

Criterion 20.2

Art. 76(3) of the APMLTF-2 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 considered. Therefore, the assessment team deems that this requirement of the standard is covered.

Weighting and Conclusion

Slovenia has overall implemented requirements on suspicious transaction reporting. However, the possibility to report transactions suspected to be linked to ML, its predicate offences and/or TF within five working days from when the suspicion arises falls short of the prompt reporting required in terms of c.20.1. **R.20 is rated LC.**

Recommendation 21 – Tipping-off and confidentiality

In its 2017 MER, Slovenia was rated C with R.21. In its 2018 FUR, Slovenia was reassessed against R.21 since the Methodology for assessing it was revised in February 2018 to clarify the interaction between the tipping-off provisions and the revised requirements on information sharing within financial groups (R.18). R.21 remained rated as C.

Since then, Slovenia undertook multiple revisions of the APMLTF-2. These changes are considered material. On this basis, R.21 is regarded as a RUR.

Criterion 21.1

When submitting data, information and documents to OMLP under the APMLTF-2, the FIs and their staff shall not be subject to the obligation to protect classified data, business secrets, professional secrecy and confidential bank data (APMLTF-2, Art. 138(1)). The same article then clarifies that this exemption equally applies to any individual, including employees and representatives of FIs (APMLTF-2, Art, 138(3)). Legislation is also silent on whether this exemption is provided if the FIs and their staff did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Criterion 21.2

FIs and their staff, including members of the management, supervisory or other executive bodies, and/or other persons shall not disclose the fact that an STR or related information is being filed with the OMLP (APMLTF-2, Art. 134(1)). However, the prohibition is only valid for eight (8) years from when the FI becomes aware of the information triggering reporting to the OMLP (APMLTF-2, Art. 134(2)). The wording used is sufficiently wide to ensure that any employee or officer of a FI is captured, independently of whether there is an employment relationship or otherwise in place between a FI and the individual concerned.

In addition, allows the exchange of information between FIs from Member States and their branches and major owned subsidiaries from third countries if the following criteria are met (APMLTF-2 Art. 135(2)):

- the branches or majority owned subsidiaries which are located in a third country implement group policies and procedures, including the procedures on exchange of information within the group;
- group policies and procedures are equivalent to provisions of APMLTF-2.

Weighting and Conclusion

Slovenia implemented requirements on tipping of and confidentiality, but some minor shortcomings remain. These include the application of time limitation for prohibition on disclosure of the fact that an STR or related information is being filed with the OMLP. **R.21 is rated LC.**

Recommendation 22 – DNFBPs: Customer due diligence

In its 2017 MER, Slovenia was rated LC with R.22, based on the following deficiencies: gap in the legal and regulatory framework related to CDD requirements, PEPs and "reliance of third parties" affect the compliance on these matters. R.22 did not undergo a follow-up review.

Since then, Slovenia undertook multiple revisions of the APMLTF. These changes are considered material. On this basis, R.22 is regarded as a RUR.

The sector of lawyers consists of attorneys registered by SBA (further referred as "covered" lawyers) and other legal advisers who are not regulated or licenced. The APMLTF-2 does not define lawyers, however, Slovenian authorities interpret it to only include covered lawyers. Slovenia has an inconsistent understanding of whether this sector falls within the scope of FATF Standards. Hence there is no regulatory framework set for these entities. This is considered as a scoping gap.

Criterion 22.1

CDD requirements detailed in the APMLTF-2 apply to DNFBPs in the same way that they apply to FIs, except as explained below.

(a) Customers identity shall be determined and/or verified when entering a casino or accessing a safe (APMLTF-2, Art.38). With respect to online gaming this is considered as the establishment of a business relationship and triggers CDD measures (APMLTF-2, Art. 22). Casinos shall carry out CDD when carrying out a transaction amounting to EUR 15 000 or more, notwithstanding whether the transaction is carried out in a single operation or in several linked operations; upon the collection of winnings, placing of a bet or both at organisers of games of chance and concessionaires, when those are amounting to EUR 2 000 or more (APMLTF-2, Art. 22(1)).

(b) Real estate entities are considered to be OEs (APMLTF-2, Art. 4(1),19(p)) and therefore are obliged to apply CDD measures. Shortcomings remain as there are no specific provisions requiring real estate agents to apply CDD requirements with respect to both purchasers and vendors of property. MIRS Guidance for real estate agents advises to apply CDD measures to both purchasers and vendors of property. Guidance, nevertheless, is not an enforceable document since the APMLTF-2 does not contain penalties for breach of guidance issued by the supervisor.

(c) Traders in precious metals and precious stones are considered to be OEs (APMLTF-2, Art.4(1),19(m)) and therefore are obliged to apply CDD measures. They are also prohibited from accepting cash payments over EUR 5 000 whether in one or multiple payments (linked transactions) (APMLTF-2, Arts.74(1) and 74(2)) and payments in other currency than Euro (Euro Introduction Act Official Journal of the Republic of Slovenia, no. 114/06). Thus, c.22.1(c) is not applicable for traders in precious metals and stones.

(d) “Covered” lawyers, auditing companies and notaries have to apply CDD for all the activities listed in R22.1(d) (APMLTF-2, Art.90). By virtue of being OEs, accountants and tax advisors shall apply Art. 22(2) to all their business activities.

(e) TCSPs shall apply CDD measures. Nevertheless, the definition of TCSP (APMLTF-2, Art.3(34)) has the following discrepancies with the definition of per the FATF Standards: (i) para (b) exempt the actual performance of a management function or the person does not assume the business risk in connection with a capital contribution in a legal entity in which he or she is formally a partner, and (ii) para (c) and (č) of APMLTF-2 definition does not include legal arrangements.

Criterion 22.2

Record-keeping requirements applied to DNFBPs are the same as for FIs. See R.11.

Criterion 22.3

PEP requirements applied to DNFBPs are the same as for FIs. See R.12.

Criterion 22.4

Requirements relating to new technologies applied to DNFBPs are the same as for FIs. See R.15, c.15.1 and c.15.2

Criterion 22.5

Requirements relating to third party reliance applied to DNFBPs are the same as for FIs. See R.17.

Weighting and Conclusion

Deficiencies identified under R.10, 15 and 17 are also applicable to compliance with R.22. Furthermore, there are shortcomings with requirements for carrying out CDD by the real estate agents; and coverage of the TCSPs activities and the lawyers. **R.22 is rated PC**.

Recommendation 23 – DNFBPs: Other measures

In its 2017 MER, Slovenia was rated LC with R.23, based on the deficiencies identified under R.18, 19 and 21. R.23 did not undergo a follow-up review.

Since then, Slovenia undertook multiple revisions of the APMLTF. These changes are considered material. On this basis, R.23 is regarded as a RUR.

The issue with the scope of the lawyers that are covered by the regulatory framework, as described in R.22 is also relevant for R.23.

Criterion 23.1

Reporting requirements applied to DNFBPs are the same as for FIs under R.20, therefore the deficiencies noted also apply to this criterion, in addition to: Auditors, "covered" lawyers, notaries, accountants and tax advisors shall report to the OMLP cases where a customer seeks advice for ML/TF purposes, no later than 3 working days after first contact (APMLTF-2, Art. 76,).

Criterion 23.2

Internal control requirements applied to DNFBPs are the same as for FIs. See R.18.

Criterion 23.3

Internal provisions dealing with higher risk countries applied to DNFBPs are the same as for FIs. See R.19.

Criterion 23.4

Tipping off and confidentiality provisions apply to DNFBPs in the same way that they apply to FIs, except as provided for under APMLTF-2, Art. 122(6). This exempts "covered" lawyers, notaries, auditors, accountants and tax advisors from a tipping off offence if they seek to dissuade a client from engaging in illegal activity. See R.21.

Weighting and Conclusion

Provisions set and deficiencies identified under R.18-21 are also applicable to compliance with R.23. Issues with a timely reporting and exemptions with the tipping off by Auditors, "covered" lawyers, notaries, accountants and tax advisors apply. The issue with the scope of the regulation of lawyers cascades through R.23. **R.23 is rated LC.**

Recommendation 24 – Transparency and beneficial ownership of legal persons

Slovenia was rated LC with R.24 during its 5th Round MER. The FATF Standards for R. 24 have undergone a revision against which the country has not previously been assessed. On this basis, R.24 is regarded as a RUR.

Criterion 24.1

(a) – (c) Based on the information provided, all LPs that can be constituted in Slovenia are subject to the requirements of R.24. The requirements under the APMLTF-2 on BO disclosure cover 'business entities' and 'entities having no equity'. Business entities would include the unlimited liability company (d.n.o.), limited partnership (k.d.), the limited liability company (d.o.o.), the public limited company or joint-stock company (d.d.), the limited partnership with share capital (k.d.d.), cooperatives and branches of foreign companies. Entities having no equity include the Economic interest grouping, GIZ, institutes, foundations, political parties, trade unions, religious communities, associations (or societies) and branches of foreign associations. Only foundations for public or charitable purposes can be established in Slovenia. This should entail that the BO disclosure requirements should be applicable vis-à-vis all LPs that can be established under the laws of Slovenia.

(d) With regard to LPs constituted under the laws of a foreign country, in so far as any such LP has a branch in Slovenia, it would be subject to the same BO disclosure requirements as any other LP, with competent authorities having access to their BO information. However, no ML/TF risk assessment has been carried out on foreign LPs to take into account the ML/TF risk they may pose to Slovenia as per the requirements of c.24.3(b).

Criterion 24.2

(a) Descriptions of different types, forms and basic features of LPs, and processes for their establishment, are set in the different laws regulating the types of LPs that can be set-up in Slovenia (Companies Act, Associations Act, Foundations Act, Institutes Act, Cooperatives Act, Freedom of Religion Act, Political Parties Act, Representativeness of Trade Unions Act, etc.). The laws are publicly available in Slovenian through the Legal Information System of the Republic of Slovenia (PISRS). In addition, information on the types, forms and basic features of LPs is found on the website of the State Portal for Business Registry (SPOT). Information on associations and foundations is publicly available on Slovenian Open Data Portal (OPSI).

(b) Information on the process for the registration of LPs and for obtaining their basic information is available online through the official governmental websites, which are publicly available and searchable.

(c) The processes for obtaining and recording of basic information for the different types of LPs are set out mainly in the BRA and CRA. The process for obtaining and recording BO information is set out in the APMLTF-2. In addition, the website of the RBO contains a general description of the process to be followed for submitting BO information. The RBO is itself accessible to competent authorities, OEs and anyone else who can demonstrate a legitimate interest.

Criterion 24.3

(a) In the 2025 NRA, within the assessments for some specific sectors and the main threats faced by the country, there is some consideration of LPs by use of limited data. There is no explicit analysis of the ML/TF risks associated with the different types of LPs that can be created in Slovenia, nor does the NRA consider the effectiveness of any mitigating measures adopted in relation thereto. Targeted risk assessments carried out by FARS (on the use of LPs for tax evasion) and OMLP (on NPOs), while contributing to risk understanding, do not address the existing gap.

(b) The current NRA does not contain any information on or assessment of the ML/TF risks posed by the different types of foreign LPs that have links with Slovenia.

Criterion 24.4

Depending on the type of LP involved, different registration processes are applicable. In the case of unlimited liability 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), European public limited liability company, limited liability co-operatives (z.o.o.), and no-liability cooperatives (z.b.o.) and institutes, an application of registration is filed through a notary or through the SPOT facility with the relevant court. Once a court issues a ruling allowing for registration, basic information and relevant documents is to be entered into the Court Registry (CR), which is part of the business registries system in Slovenia and is managed by AJPES. The AJPES also assigns each LP so entered a main activity code, the institutional sector code, a business registration number and a unique identifier. Cooperatives, which are traditionally established in the fields of agriculture and forestry, must register their activities under the same rules as companies. Economic interest groupings are formed by one or more existing companies.

In the case of foundations, the decisions whether to allow the constitution of the LPs are made by different Ministries depending on the activity to be carried out by the given foundations. The decision is then communicated to the Ministry of the Interior for the registration in the respective register. The decision to register an association is taken by regional administrative units which then communicate the necessary information to the Ministry of the Interior to populate a Central Register of Associations. Other LPs are registered by different Ministries (e.g. trade unions are registered by the Ministry for Labour in a Register of Trade Unions).

All registers are publicly accessible. Following registration in a primary register as described above, every entity is to be entered into a secondary register, the SBR, within eight days of their primary registration. The same applies for registration of any changes to the LPs. For businesses of sole proprietors and natural persons (e.g. landlords), the SBRB serves as the primary register. The SBR is therefore a central database containing information about all 'business entities' involved in a profit or non-profit activity with principal place of business located in Slovenia, as well as information on their subsidiaries and other divisions performing business activities in the country. It is managed by AJPES.

For companies, the information that companies, institutes, associations and foundations must submit to registering authorities and the data that is to be entered in the respective register this is set out under Art. 4 and Art. 5 of the CRA, complemented by the provision under the Companies Act as to what needs to be submitted for registration. The information that needs to be provided reflects the information referred to under this criterion.

For associations, the Societies Act sets out what information is to be presented with an application for registration (Art. 18) and also provides for there being a Register of Associations (Art. 46). The data entered in the Register of Associations is specified in the Rules on the Register of Associations, the Register of Branches of Foreign Associations and the Register of Associations in the Public Interest (Official Gazette of RS, No. 5/07, 56/08, 64/11 in 21/18 – ZNOrg), namely: personal name, social security number or date of birth and gender, citizenship and address of permanent or temporary residence of the representatives of the association, method of representation, limits of powers of representation, change of representatives of the association, change of method of representation, change of limits of powers of representation and date and number of the decision on their change and change of personal data of the representatives and date and number of the decision, if a decision has been issued on the change.

The information that is registered for companies, associations, foundations and institutes is publicly available online from the SBR free of charge or upon request pursuant to Art. 5 of the Access to Public Information Act.

Criterion 24.5

a) A company is to retain records corresponding to most of the basic information required under this sub-criterion in line with Art. 4 of the Register of Companies Act. However, Art. 4 makes no reference to whether the information to be retained also extends to the company's statutory documents.

(b) - (c) Companies are not obliged to maintain registers on shareholders/members/partners, but this information must be submitted to the CR and updated upon any change within three days thereof (CA, Art. 478). The only exception is in the case of public limited companies, which is to itself retain a share register with the relevant information as required by criterion 24.5(b).

An LLC is formed by a contract, the memorandum of association, which includes information on each member, their capital contributions, holdings and associated voting rights (CA, Arts. 474, 478, 482, and 506). An unlimited company is established by means of a contract of partnership between company members. An application for registration is done by all members and includes the name of each company member. Unless agreed otherwise, members shall make equal capital contributions (CA, Art. 76-78; Chapter 27, Code of obligations on memorandum of association). A limited partnership is formed by a partnership agreement (CPA, Art. 135, 136, 137). Limited partners are not entitled to conduct the partnership's business. A notification for entry in the register includes 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 CR and available through the SBR.

The books of shares for public limited companies are held within the central registry of holders of dematerialised securities maintained by the CSCC together with the holder's name and address (BESA, Art. 182, 235 CA, Art. 14(3), 25(1)). 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 SBR.

Associations must have founding acts that stipulate regulating powers. There is no explicit obligation in the law to maintain information on membership. Authorities advised that it is self-evident that an association must keep a list of members, given that management decisions must be made by its members united in the general assembly at least once a year (AA, Art. 1(2) and 13). 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 CR (CRA, Arts. 3 and 4).

Criterion 24.6

Slovenia has adopted several measures to ensure that competent authorities have access to BO through a number of sources, including the LP itself, the RBO, and OEs. BO is defined as a natural person who ultimately owns or supervises or otherwise controls a customer, or a natural person on whose behalf a transaction is carried out or services performed (APMLTF-2, Art. 40). This definition is in line with the standard. The BO definition of corporate entities and entities with no business shares (such as associations, institutes and foundations) refers to individuals who would have set-up the LP or who would otherwise be its legal representatives, and also allows for the inclusion of other individuals as BOs should these be detected by the OE (APMLTF-2, Art. 43).

Slovenia’s multi-pronged approach includes the following:

(a) Companies have an obligation under Article 45(1) of the APMLTF-2 to obtain their BO data. In line with Article 150(18), this includes an individual’s full name, permanent and temporary residence, date of birth, nationality, tax identification number and on what basis the individual has been determined to be the BO of the LP. Companies are obliged to ensure that this information is kept accurate (APMLTF-2, Art. 45(4)), and to update the information at every data modification. However, no timeframe is set for companies for updating the information.

Companies must make the BO information available to law enforcement bodies and supervisory authorities (APMLTF-2, Art. 46(1)). The term ‘supervisory authorities’ is defined under Art. 152 of the APMLTF-2, whereas authorities have advised that the term ‘law enforcement bodies’ refers to the Police and the Prosecutor’s Office. The same provision then binds companies to make the BO information available to OEs for CDD purposes.

(b) (i) Art. 48 of the APMLTF-2 provides for the setting up of a RBO, managed and administered by the AJPES. The RBO is close to being fully populated.

(b) (ii) OEs are another source of BO information. Although there is no legal requirement for Slovenian business entities to have a relationship with a Slovenian OE, the overwhelming majority (95%) do have a local bank account. For the process of identification of BO within CDD, see further under R.10.

Criterion 24.7

LPs have to retain information on an individual who ceases to be a BO thereof for five years from when the given event occurs (APMLTF-2, Art. 45(6)). The same period applies with regards to LPs that are undergoing proceedings relating to winding up or a status change "without a known successor", i.e. where the legal obligations of the LP are not to vest in anyone else. The court or other body overseeing the winding-up process is to order that the BO data be provided for the five-year period (APMLTF-2, Art. 45(7)).

BO information held by the SBR is to be publicly available for five years after the LP ceases to exist and for up to thirty years for competent authorities (APMLTF-2, Art. 50(3)).

For the retention period applicable to OEs refer to R.11.

Criterion 24.8

The registering courts (for companies and institutes), administrative units (for associations) and ministries (for-foundations) verify whether information submitted is complete and whether conditions for establishment and registration have been fulfilled (CRA, Arts. 29-30, 34; AA, Art. 19; FA, Art. 11). In case of incomplete information or unfulfilled conditions, applicants are notified and can complete the application within a certain deadline or it is otherwise rejected. Notaries are OEs when they assist clients in transactions for establishment and management of companies and management of shares (APMLTF-2, Art. 90), and must verify the identity of clients as part of CDD measures.

Companies and institutes must notify the court of changes in the registered basic information within 15 days (CA, Art. 47 and 48(3); CRA, Art. 3(3); BRA, Art. 19). For public limited companies, transfers of shares must be recorded in the share register (CA, Art. 236 (3)) maintained by the CSCC. Changes in the entries of persons in the share books are performed by the CSCC on a daily basis following the transfer of shares (BESA, Art. 25(2)). 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 (AA, Art. 20(1)). Changes in the data registered by foundations must be reported within 30 days to the registering ministries who approve the change (FA, Art. 17-18).

With regards to BO information, one key source is OEs who have to determine who is the BO of their customers and keep this information up-to-date.

Slovenia has also implemented a series of measures to ensure that the BO information held in the RBO is adequate, accurate and up-to-date. The data to be entered on a BO is adequate and comprises an individual's personal name, address of permanent and temporary residence, date of birth, tax identification number, citizenship, on what grounds an individual has been determined to be the beneficial owner, and date of entry and deletion of the beneficial owner from the register.

For the sake of accuracy, information on individuals is lifted from the Central Population Registry or from the TR, which ensures that the identification data is correct at registration stage but also on an on-going basis as the RBO is automatically updated whenever changes are made in the Central Population Registry or to the TR.

However, a number of foreign nationals not resident in Slovenia identified as BOs may not be present in either the Central Population Registry or the TR. In such cases, reliance is made on measures carried out by the LP itself and on any CDD measures applied by an OE following disclosure to the RBO. No additional checks are carried out to independently verify the accuracy of any such information entered in the RBO. Any discrepancy that may eventually be noticed, be it from the registrar, supervisory authorities or OEs, is actioned by the OMLP who, together with the FARS, are also responsible to supervise LPs' compliance with their BO disclosure obligations and the correctness and timeliness of information in the RBO and take the necessary enforcement action (APMLTF-2, Art 152(3)). The supervisory procedure by the OMLP and FARS is an administrative procedure for which all the provisions of the General Administrative Procedure Act and Inspection Act apply. The timeframe for resolving the issue is 2 months.

BO information is to be entered into the RBO within eight (8) days from the registration of the LP in the SBR or in the TR as applicable. However, there is no mechanism to ensure that the registration in the RBO actually takes place. There is the check carried out by OEs at on-boarding stage, which would therefore entail that a LP who has not disclosed its BO cannot benefit from the services of the OE. However, (i) even though all LPs seem to have a touch point with an OE at a certain point, it is not a given that all LPs will be serviced by an OE; and (ii) ensuring that changes are reported on time would be dependent on the frequency and timing of when OEs review and update their CDD data, information or documents.

The entry is to be done by the LP itself, except for single member LLC where the single member is automatically construed as being the BO. It is left to the single member company to include in the RBO any other individuals that may have been determined as its BOs within fifteen days.

LPs that are listed on a regulated market that is subject to disclosure requirements that provide suitable transparency of ownership information in conformity with EU legislation or subject to the equivalent international standards are exempt from the obligation to enter BO information onto the RBO.

The RBO has no powers to conducted checks to ascertain whether the individuals being reported actually qualify as BOs or whether someone else needs to be so reported. Discrepancies may be noted by competent authorities during their supervisory activities, in which case these are dealt with in the same manner as described earlier on for discrepancies in identification details of anyone reported as a BO.

OEs that consult the RBO are also obliged to flag any inaccuracies they notice (APMLTF-2, Art 47(10)).

Criterion 24.9

The general powers of the OMLP to request CDD information from OEs in case of grounds for ML/FT suspicions depends on the extent to which an LP has a business relation with a Slovenian OE (APMLTF-2, Art. 99-100). Furthermore, in the case of suspicions, the OMLP has the power under Art. 102 APMLTF-2 to require from any natural or legal person under Slovenia's jurisdiction to submit data, information and documents needed for detecting and proving ML, FT or related predicate offences, which could include BO information. The deadline to provide information from OEs is 5 days and – 15 days for any other public or private law entities from receipt of any such request. In either case, the OMLP can set a shorter time limit if necessary. A 15-day window for other public and private law bodies would not in itself ensure rapid access to the information referred to under this criterion. However, the ability to request information in this manner is more of a fail-safe provision, as the OMLP has advised that it already has direct electronic access to data held by an extensive number of public authorities (APMLTF-2, Art. 149(6)).

Powers of LEAs under the CPA to obtain records during 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 SBR and CSCC Register that is not publicly available. This includes ID-numbers and other personal data of shareholders, authorised representatives and members of the boards.

Art. 46(1) of the APMLTF-2 imposes an obligation on LPs to provide their BO data when required by LEAs, the courts and supervisory bodies 'without delay'. In addition, under Art. 51(4), LEAs, the courts and supervisory authorities including the OMLP have free direct electronic access to all actual BO data entered in the RBO. The entities can look for BO information by using a combination of full name and tax identification number, full name and date of birth or a combination of full name and address of permanent residence entered in the RBO.

As to the availability of basic and BO information within the course of public procurement, there is no legal requirement to disclose BO. However, the information on the SBR is accessible to the general public and is therefore accessible to authorities and others involved in public procurement. This is not the case with information within the RBO. State bodies have direct free electronic access to all data on in the RBO when deciding on the rights of entities that have a financial impact on the state budget. Authorities have confirmed that this includes also bodies responsible for public procurement purposes (APMLTF-2, Art. 51/10). Public procurement authorities need to demonstrate a legitimate interest to access BO information though this does not seem to pose a limitation in practice.

Criterion 24.10

The 2025 NRA did not consider any of the ML/TF risks associated with any foreign LPs present in Slovenia. This notwithstanding, a branch of a foreign LP has to equally disclose BO information to the RBO, even though it does not enjoy legal personality. This entails that what has been stated above is equally applicable to branches of foreign LPs.

BO information on foreign LPs who may have links to Slovenia, even though without a physical presence in the form of a branch, can still be available to competent authorities through a number of other means. The interconnection of EU/EEA BO registers should allow competent authorities within individual EU/EEA Member States, including Slovenia, to access BO information retained in participating BO registers. With regards to whether this information can be considered as adequate, accurate and up to date, much will depend on the quality checks carried out by the respective registry. However, this would only cater for those foreign LPs that are established in other EU/EEA Member States.

BO information of LPs established in a non-EU/EEA Member State could be available through other means. To the extent that the LP has established a business relationship with an OE in Slovenia, the BO information would be available through the OE. A question may arise where the only touch point between the foreign LP and an OE was through the carrying out of an occasional transaction. In such instances, it may not be possible to obtain adequate, accurate and up-to-date BO information on the foreign LP even though it may still, for example, hold immovable property within the country, as there would be no continuous relationship between the foreign LP and an OE.

In addition, the OMLP, the supervisory authorities and LEAs can make use of their channels to obtain any such information from their counterparts abroad though this may not necessarily always result in the timely access to adequate, accurate and up-to-date BO information.

Criterion 24.11

The information set out under c.24.5(a) is publicly accessible. In addition, all OEs, supervisory authorities and LEAs have access to the RBO (APMLTF-2, Art 51).

Criterion 24.12

(a) There is no outright prohibition against the issue of bearer shares under Slovenian law. However, individuals holding shares in a private company have to be always identified, be it at subscription stage or when these are acquired through a transfer. On the other hand, in the case of public limited companies, Art. 175 CA stipulates that shares can be made out to the bearer. However, this provision is rendered inapplicable due to the obligation to issue any shares in a public limited company in a dematerialised form. No shares can be so issued unless whoever is subscribing to the shares is identified and any transfer thereof is only effective to the extent that the transfer is registered by the CSCC. Authorities have advised that bearer share warrants cannot be issued under Slovenian laws.

(b) (i) Art. 175 CA stipulates that shares can be made out to the bearer when it comes to public limited companies. However, Art. 182 CA adds that all shares must be issued in book-entry form in line with the provisions of the Book Entry Securities Act. The CSCC have advised that 'book-entry form' means that shares must be issued in dematerialised 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 not doing so will effectively result in the cancellation of those shares. The Book Entry Securities Act required public limited companies that had previously issued bearer shares to allow for a 30 – 90-day period within which any such bearer shares had to be exchanged for their equivalent in dematerialised form, effectively requiring the holder to register. Not only did this entail that no rights, other than the right to exchange the bearer shares, could be exercised once a public limited company gave notice of its arrangements for the exchange to take place, but the lapse of an overall transitory period resulted in the cancellation of any bearer shares that may not have been so exchanged.

(ii) to (iii) – Given the application of (i) above, the measures set out under (ii) and (iii) are not relevant.

Criterion 24.13

Nominee shareholdings are expressly regulated only in the context of dematerialised securities held by brokerage companies under FIMA through clients' accounts. Brokerage companies can either keep securities on a personal account opened for a client (FIMA, Arts. 296(1) and (2)) or they may keep dematerialised securities on fiduciary accounts only on behalf of covered lawyers, notaries, legacy custodians, special custodians, insolvency managers and other persons providing custodian services when it becomes necessary for these professionals to hold shares under nominee on behalf of their own customers (FIMA, Art. 296(4)). In the latter case, holding shares under nominee assists with the lawful and transparent management of dematerialised securities. However, covered lawyers and notaries can have shares on fiduciary accounts only on a temporary basis for the execution of a specific transaction for clients. It is also limited in time as any such arrangement can only last twelve months, though the SMA may allow for its extension where a case is made for an extension to be granted (e.g. delays in legal proceedings).

Information on the type of the account, and indirectly the holder who is the nominee, is available to the brokerage company who operates the account, to the CSCC and to the issuer of the securities.

Brokerage companies are obliged entities under the APMLTF-2 and thereby also required to identify and verify the identity and BO of their customers prior to opening a client's account, as per Art. 297 FIMA. In the case where the client's account is opened upon request of a professional as described above, information on the underlying customers would be known to the lawyer or notary concerned as any such activity triggers CDD obligations on their part.

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 (FIMA, Arts. 105, 117-120, 134).

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 recognised; therefore, in case of "fiduciary" holding of such shares Art. 50(1) of the Code of Obligations would apply which provides that fictitious contracts are void inter partes.

Nominee directors are not recognised under Slovenian law. While there is no outright prohibition against nominee directors, a judgement of the Supreme Court has confirmed a decision of a lower court whereby the formal legal representative of a LP and a shadow director were deemed to be equally liable for the decisions of the LP, independently of whether or not the shadow director was formally recognised as such.

Criterion 24.14

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 CR of any changes in registration data (CA, Art. 685 (1)). 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 1 000-6 000 for micro companies. Responsible persons can be fined between EUR 500 and 4 000 for these offences (CA, Art. 685 (2)). The same range of fines can be imposed on public limited companies for not issuing shares in book-entry form (CA, Art. 685 (1) point 7). In addition, the Minor Offences Act, also allows for reprimands and warnings to be issued. When a company fails to update its registered address the company may also be struck off; inactive companies may be equally struck off (Financial Operations, Insolvency Proceedings and Compulsory Dissolution Act, Art. 427(1) point 2)). In case of submitting false documents to support registration applications, Art. 251 of the CC provides for two years of imprisonment for forgery of documents with criminal intent. The fines are to be imposed by the Ministry for Economy but the process and time limits applicable are not clear. Nor is it clear how the discretion allowed in determining the actual amount of a penalty is exercised.

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 (AA, Art. 53(2); FA, Art. 35(2); BRA, Arts. 19, 25). Foundations can also be fined for failure to submit their regulations to the competent authority within three months (FA, Art. 35(3)). Responsible persons of associations, foundations and institutes can be fined EUR 125, EUR 200, and EUR 200-400 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).

With regards to failure to comply to requests for information from OMLP, the APMLTF-2 provides for sanctions running from EUR 6 000 to EUR 120 000 for LPs (APMLTF-2, Arts. 178(2) and (3)) and from EUR 400 to EUR 4 000 for the legal representative of any such LPs (APMLTF-2, Art. 178(5)). This should cater for both a complete failure to reply to any such request as well as to the receipt of late replies.

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 (FIMA, Arts. 168, 529, 530).

With regard to the CDD requirements which form the current mechanism to obtain BO information, sanctions are available under the APMLTF-2 (see R.35).

As regards LPs, failure to correctly abide by their obligations relative to the identification, disclosure and reporting of their BOs, can result in a penalty as per Art. 181 APMLTF-2. The value thereof varies depending on the revenue that the LPs would have generated in the previous two financial years as resulting from its respective balance sheet as follows:

Revenue	Penalty
Up to EUR 700 000	From EUR 3 000 up to EUR 30 000
Over EUR 700 000 but not more than EUR 8 million	From EUR 6 000 up to EUR 60 000
Over EUR 8 million	From EUR 12 000 up to EUR 120 000

Considering the minimum amounts that can be imposed vis-à-vis the overall revenue of the LP, it is not a given that the available range of penalties can be considered as proportionate and dissuasive. In particular, no non-pecuniary sanction seems to be applicable in situations where the LP fails to abide by its obligations under the APMLTF-2. The same can be noted with regards to the penalties applicable to (a) individuals like the BO who fails to provide a LP with the necessary information and (b) the entity's legal representatives. Set at EUR 400 to EUR 2 000, these amounts are quite minimal and cannot be considered as presenting the necessary degree of effectiveness or dissuasiveness to ensure compliance with the obligations, bearing in mind as well that the phenomenon of the 'straw-man'. Moreover, the Minor Offences Act provides that where one pays a fine within the stipulated timeframe without having recourse to the courts, the fine is decreased by as much as 50% (Art. 57c).

Administrative penalties are imposed by the OMLP or the FARS, but the process and time limits are not clear. Nor is it clear how the discretion allowed in determining he actual amount of a penalty is exercised.

Criterion 24.15

(a) The law does not impose unduly restrictive conditions on the exchange of information between Slovenian competent authorities and their counterparts, there being restrictions only for the OMLP in exchanging information with non-EU/EEA counterparts. In such cases, the OMLP may refuse to exchange information where the non-EU/EEA FIU does not provide guarantees concerning data protection and on the use to be made of the information provided, or where the transmission of information would be considered as being contrary to the principles underlying Slovenia's legal order (APMLTF-2, Art. 115(5)). These restrictions do not seem to be applicable in the case of supervisory authorities. Of particular interest is the situation involving the tax authorities where the exchange of information can only take place within the context of a treaty or EU legislation, i.e. it does not seem that there is the possibility of exchanging information with counterpart authorities if there is no such framework in place. The Public Prosecutor's office and courts can handle incoming requests for assistance, which may relate to BO information. See also the analyses for R.37 and R.40.

(b) – (c) Most basic information, including information on shareholders, is publicly accessible. Should shareholding information be held in dematerialised form in the CSCC, competent authorities would need to exercise their powers to obtain access thereto.

(d) Art. 52 of the APMLTF-2 limits the ability of the OMLP and AML/CFT supervisory authorities to only exchange data, information and documents on BO with their counterpart authorities situated in EU Member States. It therefore suggests that any information obtained through the RBO cannot be used in replying to a request for information from a counterpart authority situated in a country that is not an EU Member State. This is addressed through the ability to exchange information obtained through other sources. This would also be applicable with regards to other competent authorities.

(e) As to monitoring quality, there is no such obligation imposed on authorities.

(f) As to keeping information in a readily accessible manner, this can be considered to be the case to the extent that this information can be obtained through the RBO. Where information has to be sourced from OEs, the information can be considered to be accessible but there may be late replies or no replies, in addition to the time that may be required for the OMLP to formulate a reply, which would not indicate that the information is 'readily accessible'.

(g) The respective laws governing the different authorities refer to the respective function to assist their foreign counterparts to obtain information (e.g. Art. 52 and Art. 115 of the APMLTF-2). However, there is limited publicly available information on how to contact the relevant agencies. Only the OMLP makes reference to its international cooperation activities in general terms on its website.

Weighting and Conclusion

The system put in place by Slovenia presents a number of positive elements. However, the 2025 NRA (a) does not consider exhaustively the ML/TF risks posed by LPs established in Slovenia; (b) does not contain any information on or assessment of the ML/TF risks posed by the different types of foreign-created LPs that have links with the country (c.24.3); and it does not consider foreign LPs (c. 24.1(d)). The obligation on LPs to retain information does not extend to the statutory documents (c.24.5(a)). Companies are not obliged to maintain registers on shareholders/members/partners (24.5(b)-(c)). There are no timeframes within which information is to be updated (24.6(a)). Information on BOs that are foreign residents is not registered in the RBO and there is no mechanism to ensure that all LPs established in Slovenia provide information on their BOs at incorporation or on an on-going basis (c.24.8). Only branches of foreign LPs have to disclose BO information to the RBO; BO information may be available through OEs but this is dependent on foreign LPs having a relationship therewith (c.24.10). Pecuniary penalties imposed for breaches of obligations relative to basic and BO information are not considered as proportionate, dissuasive and effective (c.24.14). In the case of tax authorities, the exchange of information can only take place within the context of a treaty or EU legislation (c.24.15(a)). There is no obligation to monitor the quality of basic and/or BO information received in response to a request for information (c.24.15 (e)). Reliance on OEs to provide BO information does not result in BO information being readily available (c.24.15(f)). There is limited publicly available information on how to contact agencies responsible for responding to all international requests for BO information (c.24.15(g)). **R.24 is rated PC.**

Recommendation 25 – Transparency and beneficial ownership of legal arrangements

Criterion 25.1

Slovenia does not recognise trusts under its laws but has taken steps to ensure that foreign trusts that are managed or administered from Slovenia are subject to disclosure requirements of basic and BO information. The disclosure requirements applicable to LPs and analysed under R.24 regarding BO are extended and rendered applicable to trusts and similar legal arrangements. The analysis hereunder shows that there are still some aspects that need to be addressed.

In so far as any risk assessment of trusts or similar legal arrangements managed or administered from Slovenia are concerned, none has been carried out to date.

Criterion 25.2 – (Not applicable)

Trusts or similar legal arrangements cannot be established under the laws of Slovenia.

Criterion 25.3

(a) In view of what has already been stated under c.25.2, this sub-criterion is not applicable.

(b) – (c) The 2025 NRA did not assess the ML/TF risks associated with trusts or similar legal arrangements which are either (i) administered from within Slovenia or the trustee resides in Slovenia; or (ii) are governed by foreign law but have sufficient links to Slovenia. The possibility of such a scenario is not excluded as indicated by the fact that the APMLTF-2 sets out provisions as to how OEs are to identify the BO of trusts and similar arrangements as well as the disclosure thereof to the RBO.

Criterion 25.4

(a) An OE, including anyone acting as or arranging for another person to act as trustee of an institution, trust or similar foreign law entity which receives, manages or distributes property funds for a particular purpose, is to determine a customer's BO (APMLTF-2, Art. 41(1)). BO is considered to cover the following:

(1) any natural person who is (i) the founder of a foreign fund, foreign institution or similar foreign law

entities; (ii) the trustee of a foreign fund, foreign institution or similar foreign law entities; (iii) the recipient of the benefit of the asset under management, provided that future beneficiaries have already been determined or can be determined; (iv) any protector that may be appointed to represent and protect interests of the beneficiaries of the proceeds of property (APMLTF-2, Art. 44(1)(a));

(2) a category of persons in whose interest the foreign trust, foreign institution or similar foreign law entity has been established and operates, where the individuals that benefit from the foreign trust, foreign institution or similar foreign law entity have yet to be determined (APMLTF-2, Art. 44(1)(b)). Art. 47(3) suggests that the identity of the individual(s) benefitting from the trust would be established at time of payout or when they exercise any rights granted to them under the terms of the trust; and

(3) any other natural person who through direct or indirect ownership or other type of control exercises ultimate control over a foreign trust, foreign institution or similar business entity established under foreign law (APMLTF-2, Art. 44(1)(c)). The collection of any such information is subject to the requirements set out in c. 10.7(b). Objects of power who are identified but in whose favour the trustee has not yet exercised its discretion are not covered. As regards situations involving the assignment of one's beneficial interest in a trust, this is not per se a situation considered in the APMLTF-2. However, Authorities have confirmed that the assignee would be considered as becoming a beneficiary and would therefore equally be covered under point (iii) referred to under (1) above.

(b) Any of the parties referred to above has to be a natural person (APMLTF-2, Art. 44). However, Art. 44 does not set out what is to happen when any one of the given parties is not a natural person but is either an LP or a legal arrangement.

(c) No reference is made to the trustee having to hold basic information on other regulated agents of, and service providers to, the trust and similar legal arrangement, including but not limited to investment advisors or managers, accountants and tax advisors.

Criterion 25.5

Trustees, as obliged entities, have to retain information collected for CDD purposes for ten years after the termination of a business relationship (APMLTF-2, Art. 142(1)). This would therefore include any information on a trust's BO which would be captured through the cross-reference under Art. 142(1) to Art. 47 of the APMLTF-2 which describes the information that is to be collected on BO in general, and therefore also in relation to foreign trusts (See R.11).

Criterion 25.6

As an OE, the trustee is subject to the same on-going monitoring obligations described under c. 10.7(b). The trustee must also ensure that updated information is entered into the RBO within eight days from when a change takes place. This requirement is applicable to trustees resident in or operating from Slovenia and to foreign trustees administering trusts that have established a business relationship with an OE in Slovenia or the registering of the acquisition of immovable property (APMLTF-2, Arts. 48(5) and (6)).

Criterion 25.7

(a) Art. 46(2) of the APMLTF-2 obliges trustees or a person in equivalent position to disclose their status and provide the OE with BO information whenever they enter into a business relationship or carry out an occasional transaction.

(b)-(c) With regards to cooperation with competent authorities, Art. 46(1) of the APMLTF-2 provides for the disclosure of BO information to law enforcement bodies, to supervisory authorities, and to OEs when the information is required for CDD. However, no indication was provided as to whether there are equivalent provisions which extend disclosure obligations to also cater for other information held by the trustee or anyone holding a similar position within a legal arrangement.

Criterion 25.8

The trustee itself is an OE and is therefore bound to collect information to identify and verify the identity of the customer and BO information.

With regards to any individuals identified as BOs, the information to be collected is adequate as it covers the full name of the individual, the permanent and temporary residence, the date of birth, the nationality, tax identification number and the ownership share or other method of supervision (APMLTF-2, Art. 150(1) point 14). In the case of a class of beneficiaries, data has to be collected on the given class.

Any such information has to be verified. Arts. 47(6) – (9) of the APMLTF-2 sets out a number of means through which this can be done, including through the consultation and inspection of business, court or other public registers or through original or certified copies of documents and other business records submitted by the customer's representative. Where this is not available, verification should be carried out on the basis of documents provided by the customer.

Information has to be kept up-to-date through the review and update, where necessary, on a risk sensitive basis in line with Art. 54 of the APMLTF-2. This provision makes reference to LPs but Authorities have confirmed that it is to be read as including also legal arrangements.

The same applies with regards to any other OE that establishes a business relationship with, or carries out an occasional transaction on behalf of a trust, including covered lawyers, law firms and notaries when assisting a client with establishing, operating or managing foundations, trusts, companies or similar legal organisational forms in line with Art. 90(1)(d) of the APMLTF-2 – the provision actually covering trusts and similar legal arrangements.

Any such trustee has to also disclose BO information to the RBO, which information is the same that is to be collected for identification and CDD purposes by the trustee and is therefore deemed to be adequate (Art. 50(1)(b) and (c), except for the data on classes of beneficiaries).

This obligation is not only applicable to a trustee that is resident or operating from Slovenia but also to a foreign trustee who either enters into a business relationship with an OE in Slovenia or otherwise acquires immovable property in Slovenia. In either case, BO data has to be entered into the RBO within 8 days from when the event occurs. In the event of a change, the information already provided has to be revised and updated (APMLTF-2, Art. 48(4)).

However, it should be taken into consideration that the shortcomings referred to under the c.24.8 are equally applicable in the case of trusts and similar legal arrangements that are reported on RBO.

Criterion 25.9

(a) BO information on trusts and legal arrangements is equally available through the RBO. A trustee, on behalf of the trust or similar legal arrangement, is subject to the same disclosure requirements as in the case of LPs. The analysis carried out regarding the RBO under c.24.8 is equally applicable here.

(b) Not applicable.

(c) OEs are another source of BO information. This mechanism is only available insofar as they service a trust or similar legal arrangement in the context of carrying out services triggering AML/CFT obligations. It is unclear to what extent this is the case. For the process of identification of BO within CDD, see further under R.10.

Criterion 25.10

The general powers of the OMLP to request CDD information from OEs in case of grounds for ML/FT suspicions is relevant in this regard, as far as a legal arrangement has a business relation with a Slovenian OE (APMLTF-2, Arts. 91-93). In the case of suspicions, the OMLP has the power to require from any natural or legal person under Slovenia's jurisdiction to submit data, information and documents needed for detecting and proving ML, FT or related predicate offences, which could include BO information (APMLTF-2, Art. 99). The deadline to provide information in both cases is 5 days but the OMLP can set a shorter time limit if necessary. Powers of LEAs under the CPA to obtain records during investigations are also relevant (see R.31). FI and DNFBP supervisors have powers to request information needed to perform supervision (see R. 27). As to the actual information they can obtain:

(a) Basic information is available on the trust or legal arrangement (see c.10.9). While the beneficial information can be considered as adequate to allow for the identification of a BO (see c.10.11), there are some limitations to the BO definition which do not ensure that information is available on all those that should be covered as BOs (see c.25.4).

(b) Residence information would have been collected as part of the identification of the trustee.

(c) This would be available for the specific assets held, managed or transacted by the given FI or DNFBP on behalf of a specific trust or similar legal arrangement.

Criterion 25.11

(a) Slovenia's regime with regards to BO information on trusts and similar legal arrangement is quite clear as to who is to be responsible for what. As outlined above, much depends on the trustee, with added obligations on the part of anyone who is the BO or represents the trust or legal arrangement, having equally clear responsibilities related to disclosing information.

(b) Most of the obligations to which trustees are subject to for BO transparency purposes under c.25.4 to c.25.7 reflect their CDD obligations as OEs. These latter requirements are subject to pecuniary sanctions under the APMLTF-2 (see R.35). However, there seems to be no specific sanction applicable to the trustee itself for the failure to disclose one's status as a trustee. The penalty for failure to notify the RBO of any information on time may be imposed on the legal arrangement itself or on the trustee as a trust's legal representative.

With regards to the legal arrangement, failure to correctly abide by its obligations relating to the identification, disclosure and reporting of its BOs can result in a penalty as per Art. 181 of the APMLTF-2. The value thereof varies depending on the revenue of the legal arrangement would have generated in the previous two financial years as resulting from its respective balance sheet as follows:

Revenue	Penalty
Up to EUR 700 000	From EUR 3 000 up to EUR 30 000
Over EUR 700 000 but not more than EUR 8 million	From EUR 6 000 up to EUR 60 000
Over EUR 8 million	From EUR 12 000 up to EUR 120 000

In addition, (a) an individual who qualifies as a BO and fails to provide a LP with the necessary information can be subject to a penalty of a minimum of EUR 400 to EUR 2 000; and (b) legal representatives of the legal arrangement can equally be subject to a penalty of EUR 400 to EUR 2 000.

Considering the minimum amounts that can be imposed vis-à-vis the overall revenue, it is not a given that the available range of penalties can be considered as proportionate and dissuasive. No other form of sanctioning seems to be applicable beyond the imposition of pecuniary ones and the issuance of written warnings or reprimands.

(c) The same penalties for failure to abide by BO obligations described under (b) are equally applicable for failing to grant to competent authorities' timely access to information regarding the trust referred to in c.25.4 and c.25.5. As such, the above analysis equally applies to this sub-criterion.

Criterion 25.12

(a) The analysis carried out under c.24.15(a) is equally applicable here.

(b) – (c) The analysis carried out under c.24.15(d) is equally applicable here.

(d) Slovenia referred to the powers its respective competent authorities are able to exercise to obtain BO information themselves. It is therefore understood that these same powers can be used by all the relevant competent authorities to reply to a foreign counterpart request for information on BO.

(e) See (b) above and c.24.15(f). While foreign authorities may make use of established channels of communications for the purposes of obtaining BO information, there is limited publicly available information in this regard.

Weighting and Conclusion

Slovenia's framework overall presents some positive elements, but there are a number of shortcomings present including the absence of a risk assessment on trusts and similar legal arrangements (c.25.3), the absence of an obligation to collect information on a trust's service providers or assets, and minor limitations on BO information (c.25.4); the absence of specific obligations on trustees to disclose information on aspects which may pose a limitation when confronted with confidentiality obligations especially under foreign law (c.25.7); shortcomings under c.25.8 and c.25.9 which may limit the extent to which BO information can be considered as accurate and up-to-date; limitations to the BO definition under c.25.4(a) have a bearing on c.25.10(a); and an overall sanctioning regime under which penalties cannot be considered as proportionate, effective and dissuasive. **R.25 is rated PC**.

Recommendation 26 – Regulation and supervision of financial institutions

In its 2017 MER, Slovenia was rated PC with R.26, based on the following deficiencies: fit and proper requirements do not apply to BO in all situations; a lack of an explicit requirement for supervisors to review periodically the assessment of the ML/TF risk profile of a FI or group (including the risk of non-compliance). In its 2021 FUR, Slovenia addressed most of the identified deficiencies and R.26 was re-rated as LC.

Since then, Slovenia amended its APMLTF-2, PSSIEMPSA, Banking Act (BA), Financial Instruments Market Act (FIMA) and Insurance Act (IA). In addition, the EBA Guidelines on the Risk-Based Approach to the Compliance Function was also revised in December 2024. These changes are considered material. On this basis, R.26 is regarded as a RUR.

Criterion 26.1

BoS, SMA, MIRS and ISA are responsible for the supervision of FIs, including for AML/CFT requirements (APMLTF-2, Art. 164). The BoS is responsible for the supervision of banks, PSPs, e-money institutions, MVTSs and exchange offices. Agents/distributors for e-money institutions and agents for MVTSs equally fall within the supervisory remit of the BOS. ISA is responsible for the supervision of insurance undertakings and insurance intermediaries, whereas the SMA is responsible for supervising securities' firms and collective investment schemes. MIRS is responsible to supervise lending and factoring. The OMLP is responsible of supervision of all OEs regardless of the existence of other sector-specific regulators (APMLTF-2, Art. 155).

Criterion 26.2

Core principles institutions shall be licensed (investment management companies under Art 126 and Art 103 of the Alternative Investment Fund Managers Act (AIFMA) and of the Investment Funds and Companies Act respectively, investment service providers under Art 197 of the Markets in Financial Instruments Act, insurance companies under Art 113 of the IA, insurance intermediary activities under Art. 543b, Art. 548 and Art. 549 of the IA; and banks under Art 115 of the Banking Act). In case of collective investment schemes it is the manager (management company) is the one who receives the license to manage an individual fund. authorised. In addition, not all investment fund management companies are subject to licensing or authorisation as there exists a special category of investment fund management companies which are subject only to registration.

Other types of FIs shall be licensed or authorised (PSPs and EMIs under Art. 34 and 162 of the PSSIEPSA respectively; and currency exchange offices under Art. 6 of the Foreign Exchange Act (FEA) (c.26.2 page 188 of MER 2017 and page 7 of FUR 2021). With regards to financial leasing and factoring, the former is subject to a permit being issued by the Ministry of Economy, Tourism and Sport whereas factoring is subject to licensing by the BoS in terms of Arts. 11 and 12 of the Act on Buyers and Servicers of Bank Non-Performing Loans.

Slovenia has adequate mechanisms for preventing the establishment, or continued operation, of shell banks. (CA, Art. 30, and a reference to BoS document on establishment of offices)

Criterion 26.3

Arts. 40 and 55 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. Art. 40(2) and 55(2) of the BA stipulates that a person is deemed not to enjoy the reputation and possess the traits required to manage a bank's operations where he is, inter alia, convicted of a criminal offence and the conviction has not yet been expunged from the records; or the individual has otherwise been charged with a criminal offence prosecuted ex officio and for which a prison sentence of a year or more may be imposed. Checks in the event of changes in the qualifying holding, management and structures, and supervisory boards, and the consequences on incompliance are regulated under Arts. 47 and 49 for management and Arts. 60 and 64 of BA.

Qualifying holders of bank shares must fulfil the conditions set out in Arts. 73 and 75 of the BA. Amongst the conditions that they must meet are 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 APMLTF-2, 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 APMLTF-2. 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.

These criteria are further elaborated upon in Guidelines issued by the ESAs on the management body, key function holders and qualifying shareholders. Special emphasis is made as to whether the individual, including BOs of qualifying shareholders, have been or are subject to criminal, civil or administrative (including regulatory) procedures and, where available, the outcome thereof. With regards to information sources, no express reference is made to information from sources from the OMLP. However, the BoS' internal procedures do require it to request information from the OMLP in case qualifying shareholding applications. The absence of any equivalent requirement for members of banks' management structures may not allow the proper detection of associates of criminal elements.

Any authorisation to acquire a qualifying holding can be withdrawn should the holder no longer meet the conditions to acquire the same (BA, Art. 296). As regards members of the management body, the BoS can reassess whether the conditions to fulfil the function are met at any point in time (BA, Art. 49) and have the relevant person removed if the conditions are no longer fulfilled (BA, Arts. 225, 303 and 305).

As regards the PIs and electronic money institutions and MVTS, the PSSIEMPSA requires the BoS to conduct Fit and Proper assessment of members of the management body of a PI and an EMI, who shall have appropriate reputation, appropriate knowledge and experience to perform payment services (PSSIEMPSA, Art. 32).

BoS shall assess holders of qualifying holdings (10% and above) for reasons of ensuring sound and prudent governance of a PI, in addition, the holders of qualifying holdings of a PI 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 PI. They shall consider the legal organisation form and activities that the holder provides, his/her financial positions and other characteristics. (PSSIEMPSA, Art. 33)

For exchange offices, per Art. 9 of FEA, a license shall be refused 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. In case of a change with meeting the above requirements, the permission will be revoked (Art. 10 FEA). The list of criminal offences narrows the scope of application of the FATF standards.

BoS is responsible for assessing the suitability of holder of qualifying holdings of electronic money institutions (Art. 33 PSSIEMPSA). The BoS may carry out lighter checks where the institution in question is carrying out 'other economic activities' (Art. 165). BoS has a degree of flexibility for where similar checks to its own may have already been carried out, though but this provision is rarely used.

The information sources considered by the BoS to assess whether one meets the necessary conditions to acquire a qualifying holding under the PSSIEMPSA or the FEA, or to be allowed to become a member of the management board or a key function holder are somewhat limited as they focus on the criminal record of the individual but does not use other sources like OMLP information that could be more appropriate to detect criminal associates.

The Insurance Act contains similar provisions regarding insurance companies. Art. 36 refers to the requirements of a qualifying holder of an insurance company which are similar to the requirements by banks and Art. 57 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 has not been the subject of personal bankruptcy proceedings and is a person of good reputation and integrity. Checks upon changes in the qualifying holding and management structures are regulated under Arts. 47, 60, 63 of the IA.

As to the information considered by the ISA to assess whether one meets the necessary conditions to acquire a qualifying holding or to be allowed to become a member of the management board or a key function holder, these include information from past authorisation and supervisory actions by the ISA itself, information from counterpart authorities, publicly available information, information from the applicant itself etc. However, this may not be sufficient to identify associates of criminal elements.

Financial service providers such as brokers and portfolio managers must fulfil the requirements set out in Arts. 182 and 184 FIMA regarding ownership and management functions and these sections refer to the relevant articles of the BA that apply mutatis mutandis. Checks in the event of changes in the qualifying holding and management and structures, and the consequences on incompliance are regulated under Arts. 185(8) and 232(3) of FIMA. Individuals may also provide investment services as brokers as long as they meet a series of conditions set out in Art. 291(2), including that the individual has not been sentenced by a final and binding judgment to a prison sentence of more than three months for a crime against property or the economy, which has not yet been expunged. Any permit so granted can be revoked inter alia should the individual in question be finally convicted of any such offence (Art. 222(1) point 4).

As regards AIFMs, fit and proper requirements concerning qualifying holding and management functions and subsequent changes are provided under the Arts. 40(3), 126, 127 and 132(1) of Alternative Investment Funds Managers Act. As regards UCITS management companies, fit and proper requirements concerning qualifying holding and management functions are provided under the Arts. 35(3), 40, 48 54-57, 63 and 454(1) of Investment Funds and Management Companies Act. In the case of collective investment schemes, there is no fit and proper requirements applied specifically to these schemes, as their nature as unincorporated partnerships implies that apart from the investors there will only be the investment manager who would have already been licensed.

The SMA has provided copies of its Decisions setting out how it assesses qualifying holders in the case of brokerage and management companies. The Decisions make significant reference to whether one has been, or is, the subject of criminal, civil or administrative proceedings. The SMA also consults OMLP whenever it deems it necessary or reasonable in the case of qualifying shareholders though it is then unclear whether this equally applies in the case of members of the management body or key function holders. The above mentioned also applies in the case of members of the management body or key function holders. In these cases, it therefore becomes doubtful whether the information considered would be sufficient to detect associates of criminal elements. Information from domestic and international counterparts is also sought by the SMA.

It should be noted that no reference was made by any of the authorities to the mechanisms in place to prevent the circumvention of the controls in place nor of any actions that are taken out of the authorities' own motions to detect possible cases where fitness and properness requirements are no longer met.

Criterion 26.4

(a) The SMA advised that IOSCO principles are implemented in the national legislation and that implementation is being regularly supervised. It has been recently involved in the IOSCO Standards Implementation Monitoring process for Principles 1 – 5[33] and Principles 6 – 7[34]. Issues have been flagged under Principle 3 as to the capacity of the SMA to attract and retain highly qualified employees.

Slovenia has also taken part in a peer review assessment carried out by IAIS covering most of the IAIS principles between 1 and 10. Though there are no country specific conclusions, the grouping which included Slovenia scored Observed or Largely Observed on the assessed principles.

With regards to the BCBS Principles, the IMF has recently concluded an FSAP for the Euro area which also took into account the degree to which the EU framework is compliant with the aforementioned principles. While the EU was considered to be Compliant or Largely Compliant with all relevant principles, it has to be

[33] IOSCO Standards Implementation Monitoring (ISIM) for Principles (1-5) Relating to the Regulator (FR/03/2023).
[34] IOSCO Standards Implementation Monitoring (ISIM) for Principles (6-7) Relating to the Regulator (FR/05/2025).

borne in mind that the exercise was focused on the Single Supervisory Mechanism in its totality and there are therefore no country specific conclusions.

(b) Other FIs are subject to supervision of the implementation of the provisions of the APMLTF-2 (Art. 152) considering ML/FT risks (Art. 153) (c.26.4 page 189 of MER 2017 and page 7 of FUR 2021).

Criterion 26.5

Competent supervisory authorities are to consider a risk-based approach when they conduct supervision (APMLTF-2, Art. 153). The following factors are be taken into account in the process of planning and conducting the frequency, scope, intensity of supervision:

(a) 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. In addition, the risk assessment methodologies applied by the BoS, the SMA and the ISA all take into account the control environment of the individual FI. In addition, in line with the EBA Guidelines on the Risk-Based Approach which are applicable to the authorities' supervisory activities, all three authorities are bound to also take into account the group-wide controls and risks;

(b) data on AML/CFT risk as they were identified within NRA;

(c) all significant data associated with the particular OE, including the information on any changes which are significant for obliged entity and its business activities (APMLTF-2, Art. 153(2)). The group aspect is also taken into account as required by the EBA Guidelines on the Risk-Based Approach.

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 when planning the frequency, scope and intensity of their supervisory activities (APMLTF-2, Art. 152(2)). Supervisory authorities shall review and update the factors taken into account in planning at least once every two (2) years, on the basis of which supervisors are to review and update their planning when it comes to the frequency, scope, intensity, and implementation of supervision (APMLTF-2, Art. 152(3)).

Regarding group risk assessments, Authorities referred to the EBA Guidelines on the Risk-Bases Approach, which are equally applicable to their supervisory activities, and are referred thereto.

Weighting and Conclusion

There are some limitations as to the quality of the checks carried out for the purposes of c.26.3. and it could not be assessed the degree to which the authorities are compliant with Core Principles (c.26.4). **R.26 is rated LC**.

Recommendation 27 – Powers of supervisors

In its 2017 MER, Slovenia was rated C with R.26. It did not undergo a follow-up review.

Since then, Slovenia amended its, PSSIEMPSA, BA, FIMA and IA. These changes are considered material. On this basis, R.27 is APMLTF-2 regarded as a RUR.

Criterion 27.1

BoS, SMA, MIRS, ISA and also the OMLP have sufficient powers to supervise and ensure compliance by FIs with AML/CFT requirements (APMLTF-2, Arts. 152, 155 and 164). Supervisors have 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 (APMLTF-2, Arts. 152, 155 and 164).

Criterion 27.2

Supervisors may leverage their existing powers to carry out AML/CTF supervision (APMLTF-2, Arts. 152, 155 and 164)). BoS has extensive supervision powers, including for conducting inspections which includes the authority to conduct on-site and off-site inspections on banks (BA, Arts. 264, 271-278). BoS also has the power to conduct on-site and offsite inspections on other PSPs (PSSIEMPSA, Arts. 246 and 249 to 253) and exchange offices (FEA, Art. 13).

ISA has adequate powers to conduct inspections of insurance companies, insurance brokers, insurance agents and ancillary insurance intermediaries (IA, Section 7.1, Arts. 271 to 284, 297 and Art. 563)

SMA has sufficient authority to conduct inspections on investment services companies (FIMA Arts. 340-358), on UCITS management companies (Investment Funds and Management Companies Act, Art. 442 and Arts. 447 to 449) and on alternative investment fund management companies (Alternative Investment Fund Managers Act, Art. 245 and Arts. 251 to 253). These inspections would also entail supervision of the collective investment schemes managed by different fund managers.

It is not clear from where the powers of MIRS to carry out any form of supervisory engagements derive.

In addition, the OMLP also has authority to conduct inspections (APMLTF-2, Art. 155).

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.

Banks are obliged to submit all data and documents which is needed for the purpose of supervision and ensure adequate access to data and documents which are maintained in electronic form (BA, Arts. 270-271, 277).

Regarding the securities sector, SMA has power to compel production of information without a court order when it comes to brokers (FIMA, Arts. 340-358). It has the same powers within the context of any other supervisory activity, including over management companies for UCITS and AIFs (FIMA, Arts. 488–495, BA Arts. 270-271, 277).

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 (IA, Art. 278). This power is equally applicable with regards to insurance intermediaries (IA, Art. 563)

It is unclear where MIRS derives its powers to compel the product of information and documents for the purposes of its supervisory activity.

In addition, OMLP is also authorised to compel production of any information relevant to monitoring compliance with the AML/CFT requirements (APMLTF-2, Art. 154(3) and Art. 159(1)).

Criterion 27.4

All supervisors have the power to impose sanctions for failure to comply with AML/CFT requirements (APMLTF-2, Art. 152(2)). These powers are considered under c.35.1 and the resulting analysis is applicable relative to FIs is applicable here too.

Weighting and Conclusion

Slovenia implemented requirements on powers of supervisors, but some minor shortcomings remain. These include: the lack of a clear legal basis for the carrying out of supervisory activities, including the power to compel the production of information and documents, by the SMA on alternative collective undertakings and their management companies; and framework that can limit the imposition of proportionate, dissuasive and effective sanctions (c.27.4). **R. 27 is rated LC**.

Recommendation 28 – Regulation and supervision of DNFBPs

In its 2017 MER, Slovenia was rated PC with R.28, based on the following deficiencies: gap with the basic infrastructure for sound regulation and supervision of DNFBPs; and weakness in regulation for application of a risk based supervisory approach. In its 2021 FUR, Slovenia addressed most of the identified deficiencies and R.28 was re-rated as LC.

Since then, Slovenia undertook multiple revisions of the APMLTF, the Market Inspection Act, the Notary Act and the Audit Act. These changes are considered material. On this basis, R.28 is regarded as a RUR.

The issue with the scope of the lawyers that are covered by the regulatory framework, as described in R.22 is also relevant for R.28.

Criterion 28.1

(a) Games of chance can only be conducted by concession holders or on the basis of permission received from the competent authority (Gaming Act, Art. 3), which is the Government of the Republic of Slovenia and under its authority the Minister of Finance. Games of chance over the Internet or other telecommunications means (hereinafter referred to as: online games of chance) may only be organised by companies that have a concession for the permanent organisation of classic games of chance or a concession for the organisation of special games of chance in casinos, namely only the online game of chance specified in the concession agreement concluded between the concessionaire and the Minister of finance. (Gaming Act, Art. 3a)

(b) Slovenia set a regulatory framework that ensures prevention of criminals from holding (or being the beneficial owner of) a significant or controlling interest, or holding a management function, or being an operator of a casino (Gaming Act, Art.3, 3a and APMLTF-2, Art 10(1-2)). However, it does not have a legal framework to ensure that criminal associates are prevented from holding controlling interests or holding management function or being an operator of a casino.

(c) FARS is responsible for supervising organisers and concessionaires organising games of chance (APMLTF-2, Art.164) and the OMLP is responsible for overseeing compliance with APMLTF-2 provisions (APMLTF-2, Art.152).

Criterion 28.2

The designated supervisory bodies responsible for AML/CFT supervision of DNFBPs are: (i) MIRS - real estate agents and dealers in precious metals and stones; (ii) the SBA - lawyers that are registered as attorneys; (iii) the CNS - notaries; (iv) APOA– auditors; and (v) OMLP – overall responsibility for all DNFBPs, plus accounting services, tax advisors and TCSPs (APMLTF-2, Art. 152 and 164)).

As noted in the Introduction, it is unclear whether other legal professionals fall within the scope of the FATF Standards as Slovenia has provided inconsistent information whether they conduct some of the activities set out within APMLTF-2, Art.90. However, there is no supervisory body for these.

Criterion 28.3

The OMLP are designated as a supervisor for all OEs in addition to designated supervisors if they exist (APMLTF-2, Art. 152).

Criterion 28.4

MIRS, SBA, CNS, APOA and OMLP are designated entities for the DNFBPs other than casinos.

(a) DNFBP supervisory authorities have sufficient powers to perform their functions, including powers to monitor compliance of DNFBPs. These include respective supervisory powers for the implementation of APMLTF-2 (MIA, Arts. 9-12; BAA, Arts. 59-65; Notary Act Arts. 109-112; Auditing Act, Arts. 9-16, 33-36, 73; APMLTF-2, Arts.152-155).

(b) There are a number of provisions that prevent criminals from holding a controlling or management function in a DNFBP. These are limited to requirements that the auditor, lawyer and notary respectively are not having a criminal conviction (Auditing Act, Art. 48; BAA – Arts. 27 and 30; (iii) Notary Act, Art. 8 and 9). In addition, OMLP may order a prohibition on conducting activities if an obliged entity (auditing companies, accounting services, tax advisory services and real estate businesses) or a member of the management of the OE or the BO of an OE has been convicted in a final judgement for a list of activities which among others include economic crime and terrorism-related criminal offences (APMLTF-2, Art. 152(b)). This only partly satisfies the requirements here. None of the provisions address the prevention of criminal associates. There are no provisions for TCSPs, lawyers that that perform services as per R.22.1(d) are not registered as attorneys, or dealers of precious metals and stones, tax advisors and accountants

(c) Sanctions available are explained under R.35.

Criterion 28.5

Supervisors shall apply a risk-based approach to supervision taking into account a number of factors (APMLTF-2, Art. 153), however not all elements of c.28.5 are covered. To note that lawyers that perform services as per R.22.1(d) not registered as attorneys are not currently supervised.

(a) when planning the frequency, scope and intensity of supervision and conducting supervision the supervisory authorities shall take into account the following: national risk assessment-based information on identified money laundering and terrorist financing; information on specific national and international risks related to customers, products and services; information on the risk of individual taxpayers and other available data; and important events or changes relating to the obliged entity’s management and governance and change in activity.

This does not amount to basing the frequency and intensity of AML/CFT monitoring on the risk understanding of the supervisor and considering the characteristics, diversity and number of the DNFBPs.

(b) there are no provisions for supervisors to take into account the ML/TF risk profile of those DNFBPs and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

Weighting and Conclusion

Slovenia continues to have gaps in its legal infrastructure for the supervision of DNBPs and does not supervise all activities within the scope of the FATF Standards. These include shortcomings in relation to the prevention of criminals and its associates from holding controlling or management functions (c.28.1(b) and c.28.4(b)) and the implementation of a risk based supervisory approach (c.28.5). **R.28 is rated PC**.

Recommendation 29 - Financial intelligence units

Slovenia was rated compliant with R.29 in the last MER. The applicable law was amended in 2022 but was not considered material enough to undertake a new analysis.

Criterion 29.1

The OMLP is Slovenia's FIU and is responsible for preventing and detecting ML/TF and predicate criminal offences. It serves as the national centre for receiving and analysing STRs and other information related to potential ML/TF/PF and predicate offences. OMLP is also responsible for the dissemination of the results of its analyses to competent authorities (APMLTF-2, Art. 94). Art. 76 of APMLTF-2 outlines the STRs disclosure requirements, in line with this criterion.

Criterion 29.2

The OMLP acts as the central body for the receipt of disclosures filed by obliged entities, including:

(a) STRs filed by obliged entities whenever there is a suspicion of ML/TF associated with a transaction, person, property or assets (APMLTF-2, Art. 76(1)) or any intended or executed transaction in respect of which the obliged entity knows or suspects that assets originate from criminal offences that could constitute a predicate crime of money laundering or relate to terrorist financing (APMLTF-2, Art. 76(4)). Reference is made to the analysis of relevant criteria in R.20 and R. 23 for further details.

(b) Reports on cash transactions exceeding EUR 15 000 (APMLTF-2, Art. 75(1)); reports on cash or cashless transactions exceeding EUR 15 000 transferred to the bank accounts of legal or natural persons from or having their residency (permanent or temporary) or registered office in a country found in the list of high-risk third countries with strategic deficiencies or with higher ML/FT risk (The list of high-risk third countries comprises the FATF, OECD, EU-TAX, UNODC lists and the EC Delegated Regulations). The OMLP receives from the Tax Authority data on any accompanied or unaccompanied import or export of cash amounting to or exceeding 10 000 EUR when entering or leaving the European Community and information on cash totalling less than 10 000 EUR when entering or leaving the European Community when there are indications the funds are linked to criminal activity (APMLTF-2, Art. 131).

Criterion 29.3

(a) The OMLP is legally empowered to request additional data and information from the obliged entities (APMLTF-2, Art. 99) and to request data needed for detecting and proving money laundering, predicate criminal offences, and terrorist financing from lawyers, law firms or notaries (APMLTF-2, Art. 100). In such requests OMLP must indicate the information required, the legal grounds for submission, the purpose of processing the data, and the timeframe within which it must be submitted.

(b) Art. 94(4) of the APMLTF-2 states that OMLP shall have timely, direct or indirect access to information held by obliged entities and public authorities, including information on the detection and prosecution of criminal offences. The OMLP can request information which is necessary for detecting and proving ML/TF and related predicate offences from lawyers, law firms, notaries, state bodies, bearers of public authority, and public and private law entities (APMLTF-2, Arts. 100 to 102). For such requests lawyers, law firms and notaries must provide a response without delay or within 5 days (APMLTF-2, Art. 99(5)). Art. 126(1) empowers OMLP to request information from the obliged entities, supervisory authorities and other state bodies and public authority organisations. Information must be provided to OMLP free of charge and within 15 days if not otherwise indicated in the request (APMLTF-2, Art. 126(4)). The OMLP has free direct electronic access to all data entered in the beneficial ownership register (APMLTF-2, Art. 51(4)) and free access to a wide range of information and databases (APMLTF-2, Art. 149(6)).

Criterion 29.4

(a) OMLP conducts operational analysis by using the information received from obliged entities and other information available to it for determining whether there are grounds to suspect ML/TF or predicate offences in relation to a transaction, person, property, or assets (APMLTF-2, Arts. 98(1) and 126(3)).

(b) Using data obtained pursuant to Art. 126 of APMLTF-2, OMLP conducts strategic analysis of trends and typologies of ML/ FT and risk assessments and publishes the results on its website, also informing the Government by a special or regular annual work report (APMLTF-2, Arts. 126(7) and 98(2)).

Criterion 29.5

The OMLP can spontaneously disseminate information and the results of its analysis to competent authorities if it considers that there are grounds to suspect ML/TF or predicate offences in connection with a transaction, a person, property or assets (APMLTF-2, Art. 110). Through Art. 111, APMLTF-2 introduces new provisions requiring OMLP to notify the competent authorities when there are grounds to suspect the commission of criminal offences prosecutable ex officio.

OMLP is as well empowered to provide information upon the reasoned request of several 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 Arts. 127-129 of APMLTF-2. Such information should be shared only through protected means of communication (Classified Information Act, Arts. 38 and 39). OMLP exchanges information with other competent authorities through authorised, official couriers (with security clearance) or through HKOM-the secure environment network ((network dedicated to information exchange within the Central Public Administration)).

Criterion 29.6

(a) The OMLP classifies and handles information according to its classification level, in accordance with the Act regulating classified information (Classified Information Act, Arts. 13, 34, 35). OMLP is bound to establish a system of security procedures and measures that render the unauthorised disclosure of classified information impossible. Among others, such measures must include protection of persons with access to classified information; protection of premises, equipment and communications; method of marking levels of classification; control and record of access to information and of its distribution (Classified Information Act, Art. 38). Pursuant to the security measures outlined in Arts. 38-39 of the above-mentioned act, OMLP follows internal rules and procedures with respect to confidential data handling. OMLP keeps a register with the persons that can handle classified information.

OMLP premises are physically and electronically protected. For security reasons OMLP has its own closed server, which is accessible only by OMLP staff with a password. All STRs received by OMLP are marked with "Restricted" confidentiality level, each STR being accessed only by a designated employee, the Head of the STR Sector and the Director. Nevertheless, information can be declassified by the Head of the OMLP.

(b) All OMLP staff must have a security clearance up to the minimum level "Restricted", since all received STRs are marked with this level of security. However, all OMLP employees must undergo security checks and get the security clearance for "secret" security level. The head of OMLP has "Top Secret" clearance.

(c) The access to the OMLP facilities and information is limited, since its premises are occupied only by its staff and are physically and electronically protected as referred under c.29.6.a).

Criterion 29.7

(a) OMLP was established pursuant to the State Administration Act, as a subordinated, yet independent authority within the Ministry of Finance. The OMLP has the authority and capacity to carry out its functions (analysing, requesting and disseminating) in complete autonomy, sovereignly and in an operationally independent way (APMLTF-2, Art. 94(3)(4)).

(b) In terms of international cooperation, OMLP can independently engage in information exchange with foreign counterparts (APMLTF-2, Arts. 113–124). OMLP can also independently exchange information with domestic authorities as presented under Criteria 29.3.b) and 29.5.5). For the purposes of exchanging data, information and documents OMLP may conclude cooperation agreements with foreign FIUs (APMLTF-2, Art. 113(5)) and other national competent authorities (APMLTF-2. Art. 12) to achieve its strategic and operational objectives.

(c) OMLP is a constitutive body of the Ministry of Finance. However, it is physically and functionally distinct from the ministry.

(d) OMLP has its own budget, enabling it to work independently. It submits its budget to the Ministry of Finance for approval, which is the decision-making authority in this regard. The budget allocated to OMLP in 2024 was approx. 1.55 million EUR. The OMLP director is appointed by the Government for a 5-year term, under the same procedure that applies to all directors of subordinated authorities within ministries, according to the Civil Servants Act. Also, the hiring procedure for the OMLP staff is the same as for any other state body in Slovenia and is carried out in line with the Civil Servants Act. The decision of appointment is taken by the OMLP director.

Criterion 26.8

As stated in the 5th round MER (par. 321), OMLP is a founding member of the Egmont Group, actively participating in its activities and cooperating with other Egmont Member FIUs since 1996.

Weighting and Conclusion

All criteria are met. **R.29 is C.**

Recommendation 30 – Responsibilities of law enforcement and investigative authorities

In its 2017 MER, Slovenia was rated compliant with R.30. The FATF Standards for R.30 have undergone a revision against which the country has not previously been assessed. On this basis, R.30 is regarded as a recommendation under review (RUR).

Criterion 30.1

Slovenia has dedicated law enforcement authorities with responsibility for ensuring ML, predicate offending, and TF investigations are properly conducted within the framework of national AML/CFT policies.

The principle investigative body for criminal offences including ML, TF and predicate offences is the Police, which operates at state, regional, and local levels. Within the General Police Directorate specialist functions have been established, the Financial Crime and Money Laundering Section (FCMLS) and the National Bureau of Investigation (NPU). The FCMLS is responsible for combating financial crime and ML at the state level, with a remit to oversee, supervise, co-ordinate and conduct analysis of general police investigations into financial crime. The NPU is tasked with investigating complex financial crimes, organised crime, corruption, and ML. TF criminal investigations are conducted by regional operational units and the NPU. All criminal investigations are supervised by prosecutors, which empowers Prosecutors to direct competent authorities to undertake financial investigations, lead and supervise criminal investigations and to initiate special, multi competency, investigation teams, which they lead and supervise.

Prosecutors within the SPO are responsible for ML/TF and predicate offences prosecutions. Within prosecutors' office, there is Specialised State Prosecutor's Office (SSPO), which has a national remit and is responsible for prosecuting 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.

At the EU level, the European Public Prosecutor's Office (EPPO) was established by EU Regulation 2017/1939. Slovenia participates in the EPPO and the EPPO investigates and prosecutes offences affecting the financial interests of the European Union, such as fraud (see EU Directive 2017/1371 for a list of offences), as well as any other criminal offence that is inextricably linked to criminal conduct that falls within the scope. All EU Member States shall criminalise the listed offences, which include money laundering involving property derived from the criminal offences listed in EU Directive 2017/1371.

In addition to investigative powers that are available to EPPO prosecutors under their respective national law, certain investigative measures and other measures are available to the EPPO under Art. 30 (1) of EU Regulation 2017/1939, provided that the offence under investigation carries a maximum penalty of at least four years of imprisonment. These include the power to track and trace objects, search and seizure, order the production of objects, documents or computer data, freeze instrumentalities or proceeds of crime and intercept electronic communications.

Criterion 30.2

Financial investigations are undertaken by the police dealing with the proceeds-generating crime (CPA Art. 148, Arts. 156 and 499). In addition, financial investigations can be initiated within the framework of civil forfeiture whenever there are grounds to believe that property derived from crime, (ACIOP, Art. 7). The SPO are further responsible for establishing and leading special financial investigation teams related ML/TF offences (ACIOP, Art. 14). Statutory provisions in the CPA, enable the SPO to conduct ML/TF investigations, regardless of where the predicate offence occurs.

Criterion 30.3

A number of competent authorities including the Police, FIU and the SPO are able to initiate financial investigations for the purposes of identifying, tracing and initiating freezing and seizing criminal property and property of corresponding value, collecting the information necessary for a decision on the temporary seizure of assets, and the confiscation of assets. The SPO may direct the police or other competent authority to initiate an investigation or may authorise an investigation on receipt of a submission from a competent authority. The SPO is responsible for leading and supervising the investigation once initiated (ACIOP, Arts. 13 and 14).

Criterion 30.4

Non-LEAs are subject to participation in joint investigations and to provide of specialist knowledge to those conducting investigations (CPA, Art. 160a; ACIOP, Arts. 13 and 14).

The authorities specifically note that regarding FARS Art. 100 (Financial Admin Act) authorises the conduct of a financial investigation in regard to their delegated responsibilities, which subject to the provisions of Art. 145(1) (CPA) are reported to the police.

Criterion 30.5

There is no dedicated anti–corruption enforcement authority in Slovenia. The investigation bodies, referred to in c.30.1 are also competent to investigate ML/TF offences associated with corruption offences.

Weighting and Conclusion

R.30 is rated C.

Recommendation 31 - Powers of law enforcement and investigative authorities

The FATF Standards for R.31 have undergone a revision against which the country has not previously been assessed. On this basis, R.31 is regarded as a recommendation under review (RUR).

Criterion 31.1

The police is required to take all necessary steps trace the perpetrator of the criminal offence, to prevent the perpetrator or participant in the criminal offence going into hiding or fleeing, to detect and secure the traces of the criminal offence and objects which may be of value as evidence, and to collect all information that might be useful for the successful conduct of criminal proceedings, the scope of which includes ML,TF and predicate offending (CPA, Art. 148).

(a) The investigative judge may order: a bank, savings bank, payment institution, electronic money institution or a branch or agent providing payment services or distributing electronic money on their behalf, or a company authorised to issue, manage or operate a virtual currency to disclose records. This, notwithstanding, may be ordered only if there are reasonable grounds to suspect that a criminal offence has been committed, is committed or is being prepared by specific, identifiable person (CPA, Art. 156).

(b) The authorities can search premises for the purpose of effecting an arrest or finding the traces of crime or objects relevant for the criminal proceedings (CPA, Art. 214(1). The same powers can be applied in relation to persons (CPA, Art. 214(2)). Searches may be executed with a search warrant issued by the court following an application form the Prosecutor (CPA, Art. 215).

(c) The LEAs can take witness statements (CPA, Art. 148).

(d) The LEAs can seize and obtain evidence (CPA, Arts. 148(2), 164, 218(1) and 220). Once at trial the presiding Judge may compel the production of evidence.

Criterion 31.2

There is a range of special investigative techniques that could be applied (CPA, Arts. 149a to 155a and Art. 156a). They include secret surveillance (CPA, Art. 149a), obtaining information on communications using the electronic communications networks (CPA, Art. 149b), monitoring electronic communications (CPA, Art. 150 (b)), control of letters and other parcels, control of the computer systems of banks or other legal entities which perform financial or other commercial activities (CPA, Art. 150(3)), and listening to and recording conversations, listening and surveillance in another person's home or in other areas (CPA, Art. 150(4)). Use of undercover agents/undercover operations is regulated by Art. 155a and covers wide range of measures to be used in such operations. However, controlled delivery is not specifically regulated under the CPA.

The above-mentioned investigative means can be used in relation to the criminal offences of ML and TF (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).

Criterion 31.3

The LEAs have timely access to a wide range of information to identify and trace criminal property and property of corresponding value. However, deficiencies identified under c.31.1(a) have a cascading effect on the authority's ability to identify whether natural or legal persons hold or control accounts. There are also no legal provisions enabling identification of assets without prior notification to the owner.

Criterion 31.4

The OMLP can disseminate all relevant information, on written request to the court, prosecutor's office or police conducting ML, associated predicate offences and TF (APMLTF-2, Art. 127(1)).

Weighting and Conclusion

Slovenian LEAs have majority of powers required by the standard. However, limitations are identified in relation to the threshold established in order to obtain records held by financial institutions (reasonable grounds to suspect that the crime was committed) which impedes investigating crimes in the early phase of detection. **R.31 is rated LC.**

Recommendation 32 – Cash Couriers

In its 2023 FUR, Slovenia addressed most of the identified deficiencies and R.32 was re-rated as LC following the adoption of revised EU regulations relating to EU controls on cash entering or leaving the EU (Regulation 2018/1672). Slovenian authorities reported that there were no changes introduces since the 2023 FUR.

Criterion 32.1

Natural persons entering or leaving the EU are required to declare accompanied cash (defined, inter alia, to include any currency and bearer negotiable instruments (BNIs)), to the value of EUR 10 000 or more (EU Regulation 2018/1672, Art. 3). This applies if the cash is on the traveller's person, in their luggage or in their means of transport. Where unaccompanied cash (including by post, courier, unaccompanied luggage or containerised cargo) of EUR 10 000 or more is entering or leaving the Union, the competent authorities (defined as customs and any other authorised authorities) may require the sender or recipient (or an authorised representative) to make a disclosure declaration within a deadline of 30 days (EU Regulation 2018/1672, Art. 4).

The regulations do not extend to cross border cash movements within the EU, as such only those movements into and out of the Union are subject to these measures. Art. 130(c) of APMLTF-2 regulates cash movements between Slovenia and other EU states, however there is still no requirement for physical cross-border movement of cash by mail and cargo within the EU.

Criterion 32.2

A written declaration is required for all travellers carrying cash to the value of 10 000 EUR or more, using a template declaration form. The obligation to declare cash shall not be deemed to be fulfilled if the information provided is incorrect or incomplete or if the cash is not made available for control" i.e. an obligation that the declaration is truthful (EU Regulation 2018/1672, Art. 3). No provisions for oral declarations have been implemented.

Criterion 32.3

For unaccompanied cash, the obligation to disclose unaccompanied cash shall not be deemed to be fulfilled where the declaration is not made before the deadline expires, the information provided is incorrect or incomplete, or the cash is not made available for control i.e. to provide authorities with appropriate and truthful information upon request (EU Regulation 2018/1672, Art. 4).

Criterion 32.4

See c.32.2 and c.32.3 above. EU Regulation 2018/1672 allows competent authorities to temporarily detain the cash in such cases (see c.32.8) but does not provide any power to request or obtain additional information from a traveller (in the case of a false declaration) or a sender/recipient (in cases of a false disclosure declaration).

Criterion 32.5

Art. 14 of EU Regulation 2018/1672 requires member states to introduce effective, proportionate and dissuasive penalties for cases where there has been a failure to comply with the declaration or disclosure requirements. Thus, each member state determines the amount and nature of any sanctions and should do so in line with Art. 14.

Administrative sanctions can be imposed by custom administration for breaching the provisions related to false declaration (APMLTF-2, Art.185(a)). The level of these administrative sanctions varies between EUR 3 000 and EUR 120 000 (for legal entities). A fine might also be imposed to the responsible person of the legal entity and individuals (up to EUR 4 000) (APMLTF-2, Art. 185(a)(5)(6)). In case of failure to declare cash - the customs authority is empowered to seize all the cash (APMLTF-2, Art.130(b)(1)). These sanctions are dissuasive and proportionate.

Criterion 32.6

The competent authorities shall record the declaration and disclosure information and make it available to the FIU of the EU Member State where the information was obtained as soon as possible, and in any event within 15 days (EU Regulation 2018/1672, Art. 9). Information is transmitted through the "Custom Information System", a database directly accessible by the FIU (Regulation 2021/776, Art.5). The FIU is also required to share the information with relevant FIUs from other EU member states in accordance with Article 53(1) of EU Directive 2015/849. All EU member state FIUs are connected to CIS.

The customs authorities are required 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 (APMLTF-2, Art. 131). 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 TF.

Criterion 32.7

Notwithstanding the requirement assessed in c.32.6, there are no EU requirements ensuring adequate coordination between relevant authorities at a national level on the implementation of R.32.

Domestic coordination facilitates consultation between the customs administration and the police including the dissemination of information regarding suspected criminality (CPA, Art.145). Cooperation between the customs administration and police is further formalised in a 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.

Criterion 32.8

The competent authorities are empowered to temporarily detain cash when the obligation to declare or disclose cash has not been fulfilled or when there are indications that the cash (irrespective of the amount) is related to criminal activity (EU Regulation 2018/1672, Art.7). The initial detention period is limited to 30 days, but this can be extended by competent authorities to 90 days in appropriate cases, where this is necessary and proportionate.

Domestic legislation, enables the Financial Administration and police to restrain cash and BNIs for an initial 30 days, which may be extended to 60 days for the purposes of conducting enquires to establish if there is evidence of ML or TF in cases where:

a) There is a suspicion of ML/TF or predicate offences AMPLFT. Art. 130(c.);

b) There is a false declaration or false disclosure AMPLFT, Art. 130 (b)(c.).

Police may in instances where there is a suspicion of ML/TF or predicate criminality seize cash (CPA, Art. 220). 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 (CPA, Art. 145).

Criterion 32.9

Art. 10 of EU Regulation 2018/1672 requires exchange of declaration/disclosure information with competent authorities in other EU member states, and Art.11 allows such exchange of such information through mutual administrative assistance with authorities in third countries (subject to conditions). Art.9(2) also requires exchange of such information with relevant FIUs in other EU member states. Under Art.13 all declaration/disclosure information (which includes information on the currency/BNI, and the identification data of the traveller/carrier) is to be retained for five years and may be further retained for an additional period of up to three years in specific circumstances. Slovenia also applies EC Regulation No. 515/97 on mutual assistance in customs matters. Arts. 113 to 118 of APMLTF-2 Law provide the modalities for the information exchange related to ML and TF internationally, including information on declaration.

Criterion 32.10

Art. 13 and recital 33 require that the use of personal data shall be carried out in accordance with EU law, and compatible with the purposes of Regulation 2018/1672. Any collection, disclosure, transmission, communication and other processing of personal data is also subject to the requirements of Regulations (EC) 45/2001 and (EU) 2016/679 of the European Parliament and of the Council. Art. 11 requires that any transmission of cash information to a third country is subject to the written authorisation of the competent authority which originally obtained the information and should also comply with national and EU law on the transfer of personal data to third countries.

All EU member states are part of an internal market, an area without internal frontiers in which the free movement of goods, persons, services, and capital is ensured (EU Regulation 1889/2005, Art. 26/2 TFEU and Preamble).

Criterion 32.11

Individuals who are carrying out a physical cross-border transportation of cash or BNIs that are related to ML/TF or a predicate offense, could be subjects to criminal sanctions (CC, Arts. 73 to 77(c) and CPA, Art. 502 to 502(e)). As for seizure/confiscation of cash or BNIs – Arts. 245 and 109 (CC) and Art. 491 to 507 (CPA) regulate this matter.

Weighting and Conclusion

In the absence of significant amendments, the conclusion of the 2023 FUR remains appropriate. R 32 is rated **LC.**

Recommendation 33 – Statistics

In its 2017 MER, R.33 was rated LC based on the deficiency identified in relation to the lack of the obligation to keep statistics on MLA. There have been no significant amendments to the legislation or the guidance subsequently and therefore, this recommendation is considered as non RUR.

Criterion 33.1

(a) STRS, received and disseminated: The OMLP are responsible for gathering statistics on ML and TF (APMLTF-2, Art. 114(5)) including the number of STRs received and disseminated. The data is utilised for the preparation of the Slovenian NRA (Art. 133) and provided on a regular basis to the EC.

(b) ML/TF investigations, prosecutions and convictions: The OMLP is required to collate and retain statistics on every ML / TF investigation, prosecution and conviction (APMLTF-2, Art. 134).

(c) Property frozen; seized and confiscated: the OMLP shall collate and produce annual statistics detailing the value of secured, confiscated, or seized illegal assets (APMLTF-2, Art. 134(1)). Further data is compiled by the SPO's specialist Expert Information Centre (EIC), which is responsible for centrally collating data relating to temporary seized and finally confiscated property from regional SPO offices.

(d) Mutual legal assistance or other international requests for co-operation made and received: The MoJ is not obligated to keep statistics on MLA. Separate data is retained by OMLP in relation to MLA sent or received on the basis of the Council of Europe Conventions 141 and 198

Weighting and Conclusion

In the absence of significant amendments, the conclusion of the previous MER remains appropriate, specifically that Slovenia meets the criterion of this recommendation, however, the legislation does not explicitly impose the MoJ any obligation to keep statistics on MLA. **R. 33 is rated LC**

Recommendation 34 – Guidance and feedback

In the 2017 MER, Slovenia was rated as C with R.34. The Recommendation has not been amended since then. The applicable laws have undergone amendments. On this basis, R.34 is regarded as a RUR.

Criterion 34.1

Guidance

Supervisory authorities, including SRBs, shall issue recommendations or guidelines regarding the implementation of the AML/CFT obligations by OEs (APMLTF-2, Art. 169).

BoS has issued a number of guidelines for FIs, including a Guidelines on the assessment of the risk of ML/TF (2022).

ISA issued guidelines for risk assessment for the ML/TF risks for the insurance sector in March 2023.

SMA issued a Guidelines for the Prevention of Money Laundering and Financing of Terrorism in March 2023.

MIRS issued Guidelines for the implementation of the APMLTF-2 for Lenders and Credit Intermediaries were issued in March 2024 and Guidelines for the implementation of the APMLTF-2 in the field of the real estate sector in June 2024.

SBA issued Guidelines regarding the implementation of the provisions of the APMLTF-2 in December 2017. This was revised on December 13th, 2017 and April 2023, after APMLTF-2 law revision.

OMLP issued Guidelines for the implementation of the Prevention of ML and TF Act for traders in precious metals and precious stones and products made from them were issued in June 2009, which was revised in 2025.

CNS in collaboration with OMLP issued a guidelines for notaries on the implementation of measures to identify the risk of ML and TF when assisting a client in the planning or execution of transactions in connection with the purchase or sale of real estate or a commercial company, managing the client's money, securities or other assets, opening custody accounts; or where they carry out financial or real estate transactions on behalf and for the account of a client.

APOA has issued guidelines for audit companies supporting them to be compliant with AML/CTF regulations, from, March 2023.

FARS issued Guidelines for implementation of the APMLTF-2. for concession operators and organisers of games of chance, in November 2017. This was revised in 2022, after APMLTF-2 law revision.

SBA adopted the guidelines for covered lawyers and law firms with regard to the carrying out of the provisions from the field of detection and prevention of ML and TF in October 2010. This was revised in April 2023, after APMLTF-2 law revision.

PCGRM issued a Guidelines for the effective implementation of restrictive measures in 2025.

Feedback

All authorities responsible for supervision of FIs have indicated that they use their supervisory engagements as a means to provide feedback to OEs. In addition, the OMLP is also to provide feedback on both the quality of the reports it receives as well as on the outcome of the analysis to which their report would have contributed (APMLTF-2, Art. 112). However, no information was provided by the FARS, SBA, CNS and PCGRM as to how this is done for their covered entities.

Weighting and Conclusion

Slovenia implemented requirements for guidance and feedback to a large extent. To give a full appreciation to the implemented measures evidence is missing as to how the feedback is provided by the BoS. FARS, SBA, CNS and PCGRM did not provide information on feedback for their covered entities. **R.34 is rated LC**.

Recommendation 35 – Sanctions

In the 2017 MER, Slovenia was rated as C with R.35. The Recommendation has not been amended since then. The applicable laws have undergone amendments. On this basis, R.35 is regarded as a RUR.

Criterion 35.1

Fines that can be imposed for violations of the law by the respective supervisory bodies (Chapter X of the APMLTF-2).

The levels of fines depend on the seriousness of the offence as follows:

EUR	Particularly grave offences committed by Fs	Particularly Grave offences by other OEs	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 or twice the amount of the pecuniary advantage derived from the infringement where such advantage can be determined*	3 000 to 120 000	1 500 to 60 000	750 to 30 000
Responsible person of a legal entity*	Up to 500 000	Up to 250 000 or twice the amount of the pecuniary advantage	400 to 4 000	200 to 2 000	100 to 1 000

		derived from the infringement where such advantage can be determined*			
Sole proprietor/Self employed	Up to 5 000 000 or up to 10% of turnover*	Up to 500 000	1 000 to 40 000	500 to 20 000	250 to 10 000

** The highest of the two.*

Regarding the range for Most Serious Offences, for Serious Offences and for Minor Offences, the actual fine also depends on the revenue of the OE for the previous two years per its balance sheet as follows:

Revenue/EUR	Most Serious offences/EUR	Serious Offences/EUR	Minor Offences/EUR
700 000 or less	3 000 to 60 000	1 500 to 30 000	750 to 15 000
More than 700 000 but nor More than 8 million	6 000 to 120 000	3 000 to 60 000	1 500 to 30 000
More than 8 million	12 000 to 120 000	6 000 to 60 000	3 000 to 30 000

The range ensures for fines to be imposed to be proportionate and effective. Authorities are guided by a series of criteria set out in law. These include the duration of the breach, any gains from the breach, damage caused, importance of the obligation breached, past compliance history, the motives behind the breach etc. In the absence of sanctioning policies and procedures on how a particular breach would be classified and how much weight to be attributed to each specific factor, it is unclear how similar cases are treated consistently, and that the applied penalty is proportionate, effective and dissuasive.

In addition, administrative penalties provided for the particularly grave offences require Authorities to show not that there was a particularly serious breach of an AML/CFT obligation but that it was particularly serious due to the amount of the damage caused or the amount of the illegal proceeds obtained, or because of the perpetrator's intent or intention of unlawful gain. This can act as a constraint on the application of proportionate and effective administrative penalties in particularly serious cases.

Breaches of AML/CFT obligations are classified as minor offences, requiring the sanctioning process to comply with the Minor Offences Act. This entails that no action can take place within two (2) years from when the breach is detected. This prescriptive period can be interrupted by the supervisory authorities but, the case has to be brough to its conclusion within four (4) years from when the breach was detected (MOA, Art. 42(1)(6)). This may be a serious limitation when dealing with more serious cases. In addition. The Act provides that if the fine is paid within 8 days before filing a request for judicial protection it will be reduced by 50% (MO Act, Art. 57c). This is applied regardless of any opposing views by the supervisory authority or the specific circumstances of the case.

In addition to the imposition of fines, all supervisory bodies can also take the following measures (APMLTF-2, Art. 152(2)): Issue an order setting out measures to remedy the irregularities and deficiencies within the time limit as specified by it; Propose the adoption of appropriate measures to the competent authority if it is relevant for another authority; Order other measures and perform acts for which it is authorised by law or any other regulation.

These measures are supervisory rather than enforcement actions and may be implemented regardless of any ongoing enforcement process. Both approaches can be used, where findings result in the determination of a breach of AML/CFT obligations. The BoS advised that on average it last between 6 months to 1 year, with the intensity and frequency of the interaction depending on the seriousness of the identified irregularity or shortcoming. While in the case of minor irregularities or deficiencies a declaration by the FI and off-site review is deemed sufficient, in the case of more serious issues the BoS not only requires written reports but also carries out a follow-up on-site visit to ascertain that the issue has actually been rectified. Similar processes are relied upon by the SMA and MIRS.

These are complemented by the BoS has power to impose supervisory measures such as order to eliminate violations (Section 9.3.1); early intervention measures (Section 9.3.2); and withdrawal of authorisation to provide banking services (Section 9.3.3) (Art. 279 and 280). The BoS can also take supervisory measures against qualifying holders (Section 9.4) and a member of the governing body (Section 95). The measures listed in Section 9.3 - BA are intended for prudential supervision, but they can be used for AML/CFT purposes as well. Similar measures can be imposed on PSPs in accordance with Chapter 14 of the PSSIEMPSA. In most cases an order to eliminate violations is used in order to inform the OE 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.

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 (IA, Art. 302(1)). This is interpreted to give the ISA powers of sanctioning AML/CFT violations as well. On the other hand, the SMA can only use its sanctioning powers under the APMLTF-2.

A violation may also result in the suspension or withdrawal of one's authorisation where the violation is deemed to be particularly serious. This would usually fall within the remit of the authorising authority (in the case of banks, the withdrawal would be determined by the ECB upon recommendation by the BoS). This is a power that can be exercised not by OMLP but by the supervisory authority that would have authorised the OE. It would also be dependent on the supervisory authority having the power to suspend such authorisation on the basis of AML/CFT violations. Supervisors shall publish information on AML/CFT violations on their web site (APMLTF-2, Art. 176). This should be on a 'named' basis unless the supervisor considers that this is not required or disproportionate due to specific grounds laid down in law.

Some supervisory authorities' sanctioning powers are defined in their sectoral Acts. A range of sanctions are set for notaries, from disciplinary measures to a fine of EUR 15 000, or the suspension of the right to practice (Notary Act, Art. 112). For auditors, sanctions range from an order to rectify violations, a reprimand, or to conditionally withdraw a licence or withdraw a licence (Auditing Act, Art. 81).

With regards to violations of obligations under R.6, fines can be imposed that range from EUR 200 to EUR 500 000 in the case of legal entities and from EUR 200 to EUR 150 000 in the case of individuals. The brackets allow room for fines to be imposed to be proportionate and effective. However, to the extent that there is no indication as to how the quantum of a fine is determined, it is not possible whether this is actually the case. In addition, it is understood that the Minor Offences Act would equally apply in this case and therefore the same issues flagged hereabove would find application.

Criterion 35.2

BoS, ISA, and SMA can sanction natural persons which include directors and senior management. Fines can be imposed on the responsible person of a legal entity as well (APMLTF-2, Arts. 178-180). The responsible person is anyone who is authorised to perform work on behalf, for the account, for the benefit, or with the means of a legal person, an individual sole trader, an individual who performs independent activities, state authority, or an authority of a self-governing local community; or anyone required to carry out due supervision aimed at preventing breaches of AML/CFT. The shortcomings in imposing fines with a possible decrease by 50% equally applies here.

For a particularly serious violation, the responsible person is also to be temporarily disqualified from acting as a director. This would usually fall within the remit of the authorising authority. This power can be exercised by the supervisory authority that would have authorised the OE. It would also be dependent on the supervisory authority actually having the power to suspend any such authorisation on the basis of AML/CFT violations. There is no equivalent ability to either have an individual perpetually barred from so acting nor would a temporary ban be applicable to officers other than directors.

Weighting and Conclusion

Authorities have a number of measures available to them to sanction both obliged entities and their officers. It is to be remarked that there are some issues with regards to fines, especially the possibility to just pay 50% of the penalty imposed. In addition, the timeframes may be somewhat too tight in terms of the applicable prescriptive period. **R.35 is rated PC**.

Recommendation 36 – International instruments[35]

In its 2017 MER, Slovenia was rated LC with R. 36, based on the deficiencies identified in the 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. Since then, Slovenian authorities informed that there were no changes, therefore the analysis provides a summary of the conclusions in these reports.

Criterion 36.1

Slovenia is party to all four Conventions listed in the standard.

Criterion 36.2

Slovenia has largely implemented the provisions of the Vienna, Palermo, Merida and TF Conventions into domestic legislation. However, some deficiencies were identified in the implementation of certain provision of these conventions.

Minor shortcomings in the ML incrimination (as noted under R.3) impact the implementation of Art. 3 of Vienna Convention, Art. 6 of Palermo Convention and Arts. 23 and 28 of Merida Convention. In addition, some minor deficiencies (as noted under R.4) in confiscation regime 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) and Art. 31 (3) Merida Convention. To a limited extent, the minor deficiency described under R.5 regarding the incrimination of all the offences in the treaties listed in the Annex to the FT Convention impacts the implementation of Art. 2(1)(a) and Art. 11 of the TF Convention.

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 minor 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) TF Convention.

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) TF Convention, and Arts. 51 and 53 Merida Convention are implemented.

Weighting and Conclusion

Most provisions of the Vienna, Palermo, Merida and TF 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. **R.36 is rated LC.**

[35] The UNCAC Implementation Review Mechanism (IRM), for which the UNODC serves as secretariat, is responsible for assessing the implementation of the UNCAC. The FATF assesses compliance with FATF Recommendation 36 which, in relation to the UNCAC, has a narrower scope and focus. In some cases, the findings may differ due to differences in the FATF and the IRM's respective methodologies, objectives and scope of the standards.

Recommendation 37 - Mutual legal assistance

In its 2017 MER Slovenia was rated LC with R.37 based on the following deficiencies: shortcomings in ML and TF incrimination could have affected Slovenia's ability to provide MLA in cases where dual criminality was required. Also, the absence of case management systems to monitor the progress on requests made through direct communication between judicial authorities influenced the rating for R.37. There have been no significant amendments to the legislation since the 2017 MER to warrant a re-evaluation.

Criterion 37.1

Slovenia is party to a range of international instruments relating to MLA, as well as to several bilateral agreements. The Act on Cooperation in Criminal Matters with the EU Member States (hereafter: ACCMEU) provides legal bases for assistance with EU Member States while CPA (Chapter 30) enables provision of the MLA to non-EU member states. The minor deficiencies in ML and TF incrimination (see R.3 and R.5) could however be an issue when responding to foreign requests for MLA in cases where dual criminality is required.

Criterion 37.2

In instances when MLA is provided based on the international treaties MoJ serves as a central authority, except for the 1990 Strasbourg and 2005 Warsaw Conventions where the OMLP acts as the central authority. Article 515(3) CPA and international treaties may allow direct exchanges between domestic and foreign authorities during criminal proceedings.

To manage and prioritise MLA requests, the MoJ uses an electronic system with deadline alerts, while the OMLP maintains a document management system for tracking forwarded requests.

Within the EU, the ACCMEU facilitates direct communication between judicial bodies and emphasises swift legal assistance. However, no case management systems were identified for monitoring such direct communications.

Criterion 37.3

The provision of MLA is not subject to unreasonable or unduly restrictive conditions.

Criterion 37.4

The CPA and other relevant legislation do not prohibit the provision of MLA if the offence involves 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.

Criterion 37.5

Relevant international agreements to which Slovenia takes part and which are in force by virtue of Art. 514 CPA 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 CPA and Art. 201 of the Court Order provide the necessary protection.

Criterion 37.6

The dual criminality principle is not applied in relation to EU member states (ACCMEU, Art.49). As concerns MLA requests originating from non-EU States, Slovenia has maintained the condition of dual criminality in relation to coercive measures.

Criterion 37.7

The requirement of dual criminality is deemed to be satisfied regardless of the offence categorisation 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.

Criterion 37.8

The competent authorities decide upon the manner of implementation of an act requested by a foreign authority pursuant to international agreements and national regulations (CPA, Art.516 (4)). Slovenia can also provide assistance to other EU countries in controlled delivery (ACCMEU, Art. 55), even if this special investigative technique is not available to LEAs in pure domestic situations. Recent amendments to the CPA limit the powers of Slovenian authorities to use certain investigative measures (see R.31.1).

Weighting and Conclusion

Slovenia mostly meets requirement set out in this recommendation. However, there are no case management systems in place to monitor progress on requests made through direct communication between judicial authorities. To a lesser extent, minor gaps in TF and ML offences could negatively affect Slovenia's ability to provide MLA in cases where dual criminality is a condition for executing MLA requests. **R.37 is rated LC.**

Recommendation 38 – Mutual legal assistance: freezing and confiscation

In its 2017 MER, Slovenia was rated LC based on the deficiencies identified under R.3, 4 and 5 which could, to some extent, have limited the cooperation that could have been provided. The FATF Standards for R.38 have undergone a revision against which the country has not previously been assessed. On this basis, R.38 is regarded as a recommendation under review (RUR).

Criterion 38.1

Slovenia has the power to identify, trace, evaluate, investigate, freeze, seize and confiscate criminal property and property of corresponding value (see R.4). When cooperating with the non-EU countries, CPA allows to use these powers when rendering mutual legal assistance in freezing, seizing and confiscating instrumentalities and proceeds derived from the criminal offence (CPA, Art. Art.516 (4)). Slovenia can provide mutual legal assistance to other countries even when confiscation order of a foreign state was brought in civil proceeding (ACIOP, Chapter VIII). However, the previsions of ACIOP apply only when the value of the assets exceeds a threshold of € 50,000.

EU Regulation 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders provides for the mutual recognition, between EU member states, of freezing and confiscation orders resulting from proceedings in relation to a criminal offence. It includes freezing and confiscation orders that apply to property that is held in the name of or owned by non-bona fide third parties. EU Regulation 2018/1805 does not provide for the recognition of requests for investigative measures or non-criminal seizure of assets. Whether "freezing" also extends to cover situations in which competent authorities take physical control of an asset is an issue to be determined by the law of the member state. For orders that concern criminal offences with a maximum penalty of at least 3 years imprisonment, and which are also listed in Article 3 of the Regulation (which mirrors the offences set out in the FATF definition of "designated categories of offences"), the order should be executed without verifying dual criminality. Otherwise, the member state can verify that dual criminality exists. Recognition and execution of freezing and confiscation orders should occur without delay

Criterion 38.2

EU Regulation 2018/1805 provides for the recognition and enforcement of freezing and confiscation orders that have been issued within the framework of proceedings in criminal matters. Requests for the recognition of freezing orders can be issued by a judge, a court, a public prosecutor or another competent authority (provided this is validated by a court/public prosecutor), for confiscation orders requests can be issued by an authority which is designated as such by the issuing State and which is competent in criminal matters to execute a confiscation order issued by a court in accordance with national law. The term "proceedings in criminal matters is not defined in EU Regulation 2018/1805, but the preamble does state that it extends to" other types of orders issued without a final conviction". The Regulation covers orders issued without a final conviction in the framework of proceedings in criminal matters. It does not cover orders that have been made in the context of civil or administrative proceedings.

When cooperating with non-EU Member States, the CPA enables Slovenia to recognise and enforce foreign orders for conviction-based confiscation, while ACIOP enables it to recognise and enforce foreign orders (from EU and non-EU States) for extended and non-conviction-based confiscation for assets of a value exceeding €50,000 (ACIOP, Art 51 (2)). The same applies to provisional measures. Nevertheless, deficiencies under c.4.5 have a cascading effect.

Criterion 38.3

Under EU Regulation 2018/1805 it is mandatory to recognise and enforce the freezing and confiscation order of another EU member state, unless the executing authority invokes one of the grounds for non-recognition and non-execution. This means that there is de facto reliance on the findings of fact in the foreign order.

Outside the EU framework, CPA provides the framework for recognising and enforcing foreign freezing, seizing and confiscation orders (CPA, Art. 516 (5)). Slovenia can provide assistance in the manner indicated by the requesting country, if compliant with the fundamental principles of Slovenian laws. There is no special provision in the CPA that conditions the enforcing of foreign orders on the conduct of a domestic investigation.

Criterion 38.4

Under EU Regulation 2018/1805 confiscation orders are only issued by a court. Freezing orders may be issued by an issuing authority, which can be a prosecutor, judge, court or another designated competent authority, such as a law enforcement authority. In the latter case the order should be validated by a court, judge or public prosecutor before making a request for recognition and execution, which implies that another authority (prosecutor, judge or court) should have the power to validate the freezing order issued by an authority that is not a prosecutor, judge or court. Under the national legislation, Slovenian courts have the power to issue seizing, freezing and confiscation orders (CC Art. 74(2); CPA, Art. 502(1)(2), 502a 502b and Art 503).

Criterion 38.5

According to the EU Regulation 2018/1805 (Art.28) management of frozen and confiscated property should be governed by the national legislation which shall include the power to sell or transfer such property. The property shall be managed to prevent its depreciation in value. Furthermore, member states are obliged to restitute frozen property to victims (art.29), and there are procedures how confiscated property is to be restituted to or used to compensate victims and also how such property is to be otherwise dealt with (Art.30). When cooperating with non-EU Member States, management, preservation and disposal of seized, frozen or confiscated criminal property in the cross border asset recovery process is regulated by CPA, Art. 506.

Criterion 38.6

(a) Article 25 of the EU Regulation 2018/1805 and several other provisions refer to communications between the requesting and requested countries. Communication is to be between the issuing and executing authorities, also with the involvement of a central authority where appropriate. Indeed, nearly every provision of the Regulation contains a clause on communication, such as who shall inform whom of action taken or not taken, what needs to happen when an issue is encountered etc. Article 25 therefore basically only adds additional communication obligations to what the Regulation already provides for in each specific Article. The Regulation does not create communication mechanisms or measures (any form of communication capable of producing a written record is, in principle, acceptable), but does state that communication should occur where necessary. The Regulation does not refer specifically to communication before a formal request is made, or to cases involving a follow up request to an initial request that is not connected to the recognition or execution of that specific request.

The national legislation sets out the possibility for the prosecutors and judges to exchange information informally with foreign authorities, including for facilitating assistance before the submission of a MLA request (CPA, Art. 516c (1)).

(b) Article 7(1) and 18(1) of the EU Regulation 2018/1805 provide that freezing and confiscation orders shall be recognized and all necessary measures taken for their execution in the same way as for domestic orders. There is no explicit provision providing for further related assistance on an initial request, without requiring a supplemental request, but the EC considers that where the execution of a request requires further measures to be taken which would also be taken to execute a domestic order, no additional request for assistance is required for those measures. Additionally, Article 18(5) of the Regulation provides that where the issuing authority has issued a confiscation order but has not issued a freezing order, the executing authority may, as part of the abovementioned measures decide to freeze the property concerned of its own motion.

The authorities may, if so, provided by an international agreement, without prior request, transmit information if it is considered useful for pre-trial or criminal proceedings to competent authorities of other States (CPA, Art. 516c).

Criterion 38.7

(a) Article 30 of EU Regulation 2018/1805 sets out how confiscated property should be dealt with. Unless there is victim/restitution or compensation, or there is a different agreement between the countries, then, where property other than money is concerned, the rules of paragraph 6 of Article 30 apply. Where money is obtained as the result of the execution of a confiscation order, paragraph 7 of Article 30 provides that:

> (a) in cases of EUR 10 000 or less, the property accrues to the requested state, and
>
> (b) if above EUR 10 000 then it is divided 50% to each state. There is no specific mention of cases involving coordinated LEA action.

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. 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.

(b) As regards sharing of costs, Article 31 of EU Regulation 2018/1805 provides for sharing arrangements in cases involving substantial costs. Cost sharing agreements are, however, not part of the mechanism for the disposal of confiscated assets unless, where in accordance with paragraph 7, member states decide to reach a different agreement to the rules set out in that paragraph and agree to also cover the sharing of costs in that agreement. In principle, cost sharing is a separate matter under the Regulation.

Besides the directly applicable EU framework, there is no domestic legal framework covering the deduction or share of substantial extraordinary costs incurred with the enforcement of a freezing/seizing/confiscation order of non-EU countries.

Criterion 38.8

Slovenia is a party to international treaties, among which 1990 Strasbourg Convention, the 2005 Warsaw Convention, the UN Convention against Corruption (UNCAC) and the Palermo Convention.

Moreover, EU Regulation 2018/1805 applies to all MS except Denmark and Ireland. All member states except Czechia, Finland, Ireland, and Luxembourg have signed and ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198).

Weighting and Conclusion

Slovenian provisional measures and confiscation regime is generally comprehensive, allowing the execution of MLA requests related to both criminal and civil based confiscation proceedings. Minor deficiencies identified under R.3 and R.5 could, to some extent, limit the cooperation that can be provided. **R.38 is rated LC**

Recommendation 39 – Extradition

In its 2017 MER Slovenia was rated LC with R. 39 based on the deficiencies in ML and TF incrimination that could further impact on the scope of application of extradition measures. Slovenia has since not made any material update to R.39 and the analysis below is a summary of the 2017 MER.

Criterion 39.1

Extradition procedure between Slovenia and other EU Member States is regulated by ACCMEU-1 which 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 of the CPA and relevant international instruments.

(a) ML and TF are extraditable offences.

(b) 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. There is a general obligation to all authorities involved in the criminal proceedings to expeditiously undertake actions if the accused has been detained, which is usually the case in extradition procedures (CPA, Art. 200).

Part II of the ACCMEU-1 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. However, there are no case management systems in place for judicial authorities handling surrender requests through direct communication in the EU framework.

(c) there are no unreasonable or unduly restrictive conditions on the execution of the extradition's requests.

Criterion 39.2

Slovenia cannot extradite its own nationals (Constitution, Art. 47). However, in instances where 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 (CPA, Art.527).

Slovenian citizens may be surrendered to member states of the EU on the basis of the European Arrest Warrant (ACCMEU-a, Art. 117). 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 (ACCMEU-1, Art.11).

Criterion 39.3

Dual criminality is a requirement for the execution of the extradition request (CPA, Art. 522 (3)) and ACCMEU-1, Art 9(1)). The condition of dual criminality is deemed satisfied if Slovenia also criminalises the conduct underlying the offence, irrespective of exact qualification of the offence. The shortcomings in the ML incrimination (see R.3), may limit possibilities to extradite to countries outside of the EU.

Criterion 39.4

Simplified extradition procedures are possible if the sought person consents (CPA, Art. 529a; ACCMEU-1, Art. 22). 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 (CPA, Art. 525).

Weighting and Conclusion

Slovenia has appropriate extradition procedures. However, some weaknesses relating to the ML offence may impact on the scope of application of these measures. Also, the judicial authorities lack a case management system for handling surrender requests through direct communication in the EU framework. **R. 39 is rated LC**

Recommendation 40 – Other forms of international cooperation

In its 2017 MER Slovenia was rated LC on R.40 based on the following deficiencies: ISA's lack of power to cooperate with non-EU counterparts and lack of procedures to provide feedback on cooperation with foreign counterparts. Also, a lack of legal provisions was found with respect to (i) Police's protection of data received from foreign LEAs, (ii) the ability of Police and Prosecution to exchange information diagonally/ with non-counterparts. Moreover, Slovenian legislation did not specifically ensure that competent authorities indicate the purpose and beneficiary authority when requesting information indirectly. The FATF Standards for R.40 have undergone a revision against which the country has not previously been assessed. On this basis, R.40 is regarded as a recommendation under review (RUR).

Criterion 40.1

Slovenian competent authorities can ensure that they can promptly provide a wide range of international cooperation in relation to ML, TF and predicate offences to their foreign counterparts (see c.40.2). Supervisors, the FIU and LEAs are able to share information both spontaneously and upon request.

At the EU level, Slovenia also cooperates in cross-border investigations and prosecutions via the European Union Agency for Criminal Justice Cooperation (Eurojust) and through cooperation in law enforcement via the European Union Agency for Law Enforcement Cooperation (Europol). Eurojust - based on EU Regulation 2018/1727 - has the tasks to support and strengthen coordination and cooperation between national investigating and prosecution authorities in relation to serious crime where that crime affects two or more member states, including in relation to money laundering activities or terrorism (Art. 3 and Annex I EU Regulation 2018/1727). Europol provides operational and strategic support to law enforcement authorities in the EU in cross-border cases of serious crime, including preventing and combating money laundering and terrorism (Art. 3 and Annex I EU Regulation 2016/794).

Criterion 40.2

Competent authorities can provide cooperation to their foreign counterparts according to the following legal framework:

a) The OMLP can cooperate based on the provisions of Chapter 6.3 of APMLTF-2. All supervisory authorities can cooperate with foreign counterparts on AML/CFT issues based on the Art. 171-172 of the

APMLTF-2. In terms of prudential supervision, Financial Supervisors can cooperate with foreign counterparts from EU Member States or from third countries on the basis of international agreements or the sectoral laws (BoS based on Arts. 16 and 23 of BA, SMA based on Art. 173, 351 to 356, 430 of FIMA and ISA based on Arts. 289 and 290 of IA). Prosecutors cooperate based on the CPA and ACCMEU-1, latter being used when cooperating with the EU Member States. Cross-border police cooperation is carried based on Police Tasks and Powers Act (Art. 117).

b) There are no impediments that would prevent the competent authorities from using the most efficient means to cooperate.

c) Competent authorities have appropriate and secure mechanisms to exchange information.

The OMLP uses Egmont Secure Web and the FIU.Net networks for the exchange of information (APMLTF-2, Art. 122). FIU.net is used for the exchange with FIUs of EU member states. The system is hosted by the EC, allowing EU FIUs to securely exchange and cross-match information for the analysis of potential cases of money laundering, associated predicate offences and terrorism financing.

The police authorities use several networks such as AMON – Informal network for AML, CARIN, Interpol I-24/7 and Europol Siena. At the EU level, Europol has developed the Secure Information Exchange Network Application (SIENA), a state-of-the-art tool designed to enable swift, secure and user-friendly communication and exchange of operational and strategic crime-related information and intelligence between Europol, member states and Third Parties with which Europol has cooperation agreements / working arrangements.

The Prosecutor's office exchanges information through Camden Asset Recovery Inter-Agency Network (CARIN), Eurojust, EJN – the European Judicial Network, ARO and AMO platforms and through Eurojust. At the EU level, Eurojust acts by opening a coordination case in the Case Management System that is regulated by Art. 23 EU Regulation 2018/1727 and operates based on processes and data protection standards set out by law.

Supervisory authorities exchange information with foreign counterparts in accordance with the confidentiality conditions specified in the Memorandums of Understanding.

However, the AML/CFT law and the sectoral legislation (BA, FIMA and IA) do not provide for the use of secure gateways for the exchange of information at international level.

For the exchange of information between financial supervisors, the European Banking Authority (EBA) provides the system eGATE that facilitates the exchange of information with competent authorities in EU member states supervising credit and financial institutions.

FARS securely exchanges tax and customs information within the EU through CCN network and AFIS-mail. Information exchanged with non-EU countries is encrypted with a password (separately transmitted) before sending.

d) All competent authorities have clear processes for prioritisation and timely execution of requests. The OMLP prioritises requests in accordance with the Egmont Principles for Information Exchange. The Prosecutor's office prioritises on case by-case bases, while police prioritises according to the date of receipt of the request "first in, first served". Supervisors generally execute all requests within the deadlines indicated by the foreign counterpart or proposing timeframe for execution of a request.

e) Information exchanged by competent authorities is processed in line with the law regulating classified information. AML/CFT and sectoral legislation is also applicable (OMLP – Art. 114(4) APMLTF-2; SMA – Art.351(6) FIMA-1, Art. 488, 488a FIMA; BoS - Art. 14-16 BA; ISA - Art.289, 290 of the IA). Information received by SMA is also safeguarded on the basis of MMoUs, point 11 (*Confidentiality*) of the IOSCO

MMoU and Art. 7 of the ESMA MMoU. FARS advised that the information exchanged internationally is safeguarded as if obtained domestically, in line with the provisions of the 5th Chapter of the Tax Procedure Act (TPA).

Criterion 40.3

In general, the competent authorities do not need bilateral agreements to cooperate with foreign counterparts. However, where needed, the authorities can negotiate and sign bilateral and multilateral agreements in a timely manner (APMLTF-2, Arts. 113(2); 171(2); 172(2), (3)). Some of these agreements were concluded by the OMLP, ISA, SMA, FARS, police, and by prosecutors.

The police and prosecutors can sign agreements (CPA, Art.160b) in the course of pre-trial proceedings, investigation or main hearings within the framework of a joint investigation team (JIT).

The police do not need to conclude bilateral agreements to cooperate with foreign counterparts (Art. 117 Police Tasks and Powers Act), however, numerous bilateral and multilateral agreements and protocols (total of 82) have been signed.

Criterion 40.4

The OMLP can provide feedback to foreign counterparts regarding the usefulness and applicability of the received data and the outcome of the analysis carried out using the information received (APMLTF-2, Art. 119). Police, ISA and SMA do not have a standard procedure for giving feedback to a foreign authority. This is however done on case-by-case basis. No information has been provided with regard to the other competent authorities (Prosecutors, and other supervisors).

Criterion 40.5

Provision of assistance by competent 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 harm its sovereignty and security. With regard to FIs, lawyers, notaries and other OEs, when providing AML/CFT data to OMLP, the obligation to protect professional secrecy shall not apply (APMLTF-2, Art. 138). The OMLP may request AML/CFT information from OEs and DNFBPs (APMLTF-2, Art. 99-100).

Criterion 40.6

The competent authorities (OMLP, BoS, SMA, FARS, ISA, Police, Prosecutors) have safeguards to ensure that exchanged information is used only for the purpose indicated in the request and by the requesting authority unless prior authorisation is given (APMLTF-2, Art. 114(4)-115; BA, Art. 16(5); FIMA, Art. 351(6) and Art. 488a(2) and IA Arts. 290 and 509; The Law on Duties and Powers of Police, Art. 117(3)(5); State Prosecutor’s Act, Art. 180(2), CPA, Art. 516c(3)).

Criterion 40.7

All competent authorities (OMLP, police, prosecutors, BoS, SMA, ISA, FARS) have the obligation to protect confidentiality and protection of data exchanged (APMLTF-2, Art. 114 (4)); State Prosecutor’s Act, Arts. 41 and 180; The Law on Duties and Powers of Police (Art. 117(3)(5)(6)) BoS - Arts. 14-16 BA; SMA - Arts. 488, 488a FIMA; ISA – Arts. 289, 290 IA; Chapter V of the Tax Procedure Act.

Criterion 40.8

All competent authorities (OMLP, police, prosecutors, BoS, SMA, ISA, FARS) can conduct inquiries on behalf of foreign counterparts and all of them except police exchange with their foreign counterparts all information obtained (APMLTF-2, Arts. 115(2) and 172; Police Tasks and Powers Act, Art. 117(2); CPA, Art. 516(4); BA, Art. 23; FIMA-1, Art. 351(7)); IA, Art. 289 (1)).

Criterion 40.9

The OMLP has legal bases to provide cooperation on ML, associated predicate offence and TF (APMLTF-2, Arts. 113 - 119), regardless of the type of the FIU seeking cooperation.

Criterion 40.10

At the request of a foreign FIU, the OMLP shall provide feedback regarding the usefulness and applicability of the received data and regarding the outcome of the analysis carried out using the information received from the foreign FIU (APMLTF-2, Art. 119).

Criterion 40.11

The OMLP has the power to exchange data, information and documents concerning customers, transactions and suspicious property linked to ML/TF, which could be relevant to the analysis of another FIU, provided that a mutual exchange of information exists in practice (APMLTF-2, Art. 115(2)).

Criterion 40.12

The OMLP is authorised to temporarily suspend a transaction, based on the request of a foreign FIU, for a maximum of 3 business days by issuing a written order. In urgent matters, exceptionally, the order may be issued orally and must be followed by a written order as soon as possible. The OMLP can send or receive suspension requests indirectly to/from foreign competent authorities, through the FIU of the requesting state (APMLTF-2, Arts. 105, 120 and 123).

Criterion 40.13

All financial supervisors (BoS, SMA and ISA) have the power to cooperate with foreign counterparts on AML/CFT issues, specifically with regard to the supervision of OEs and in order to facilitate supervision (APMLTF-2, Arts.171-173). Financial supervisors can exchange information with foreign counterparts with regard to prudential supervision based on sectoral laws and concluded international agreements (SMA based on Arts. 173, 351 to 356, 430 of FIMA, BoS based on Arts. 16 and 23 of BA and ISA based on Arts. 289 and 290 of IA).

Criterion 40.14

The OMLP and other supervisory bodies are able to exchange with foreign counterparts information available to them, including information held by financial institutions (APMLTF-2, Arts. 171, 172 and 173). In addition, regarding cooperation in the field of prudential supervision, sectoral laws apply. BoS can disclose information to third parties (BA, Art. 16, 20 and 23) and ISA can exchange information with supervisory authorities of EU Member States (IA, Art. 289) and with counterparts from third countries by concluding a cooperation agreement (IA, Art. 290). The same applies for SMA (FIMA, Art. 351).

Criterion 40.15

Supervisory authorities can exchange all types of information which is necessary for the effective supervision of OEs, including OEs that are part of a group. At the EU level, competent authorities supervising credit and financial institutions concluded an agreement on the exchange of information with the European Central Bank acting as a prudential supervisor. Information exchange can extend to prudential and AML/CFT information, including material weaknesses int the AML/CFT governance, systems and controls framework.

For supervisors in the EU, the AML/CFT Colleges Guideline36 create a common framework to support effective oversight of cross-border groups from an AML/CFT perspective and also from a more general prudential perspective. Specifically, AML/CFT colleges provide a permanent structure for cooperation and information exchange between supervisors from different member states and third countries that are responsible for the AML/CFT supervision of the same firm. The guidelines set out the rules that govern the establishment and operation of these colleges, and structure the exchange of information between AML/CFT and prudential supervisors, who will be invited to participate in AML/CFT colleges as observers.

a) Supervisors (BoS, SMA, ISA) can exchange regulatory information (BA, Art. 23; FIMA, Art. 351 and IA, Arts. 289-290).

b) Supervisors (BoS, SMA, ISA) can exchange prudential information (BA, Art. 23; IOSCO MoU and bilateral MoUs and FIMA, Art. 351; IA, Arts. 289 and 290).

c) Supervisors (BoS, SMA and ISA) can exchange AML/CFT information (APMLTF-2, Arts. 171 and 172).

Criterion 40.16

Supervisory authorities can cooperate with EU and third countries and exchange all information that could facilitate the group supervision of OEs (APMLTF-2, Arts. 171 and 172). Moreover, pursuant to sectoral legislation, SMA has full capacity to exchange information with competent supervisory authorities from EU MS/third countries, using all its powers to obtain data and information required by the latter (FIMA, Art. 351 (5)(7)), while BoS and ISA have full powers only with regard to EU counterparts (BA, Art. 23, IA, Arts. 289, 290).

With regard to third countries, the extent to which BoS and ISA can exchange information with counterparts is not expressly covered by the provisions of Art. 23(6) of BA and Art. 290(1) of IA. They can conduct inquiries on behalf of foreign counterparts according to cooperation agreements concluded.

Criterion 40.17

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 (APMLTF-2, Art. 115). 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, TF and related predicate offences. (APMLTF-2, Art. 114).

SMA can disseminate information acquired from a competent supervisory authority of another MS/ third country only with the consent of the latter (FIMA, Art. 351(6)). The same applies for ISA, according to the provisions of Art. 509 of the IA. BoS can also disseminate received information only with the consent of the foreign supervisory authority (BA, Art. 19(2)).

Criterion 40.18

Police can exchange information related to ML, associated predicate offences or TF with foreign counterparts for both - intelligence and investigative purposes (Police Task and Power Act, Art. 117 and Organisation and Work of the Police Act, Arts. 18, 20 and 38).

At the EU level, exchanges of information with individual law enforcement authorities are complemented by number of systems and databases that can be used by the Slovenian competent authorities to access data, in

[36] Joint guidelines on cooperation and information exchange for the purpose of Directive (EU) 2015/849 between competent authorities supervising credit and financial institutions, published by the European Banking Authority on 16 December 2019 (JC 2019 81).

line with the established access right: Schengen Information System (SIS), The Entry/Exit System (EES), Eurodac, European Travel Information and Authorisation System (ETIAS), European Criminal Records Information System (ECRIS-TRN), police records in line with Prüm II Regulation.

Slovenia has also ratified the Convention implementing the Schengen Agreement of 14 July 1985. Police cooperation is defined in Chapter 1 of the 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.

Also, Police, prosecuting and judicial authorities are able to exchange domestically available information with foreign counterparts according to the provisions of ACCMEU-1 and CPA, Art. 515(3).

Criterion 40.19

(a) LEAs are able to exchange domestically available information for intelligence and investigative purposes with the competent authorities of another EU MS (ACCMEU-1, Arts. 52,53 and 54) and with competent authorities of non-EU countries (CPA, Art. 516c). This includes the identification and tracing of the proceeds and instrumentalities of crime. Also, the Slovenian ARO Contact Point, which operates within the Supreme State Prosecutor's Office, cooperates with EU counterparts according to Council Decision 2007/845/JHA. Furthermore, Slovenia can internationally cooperate according to the provisions of Arts. 48-54 of ACIOP.

b) While Slovenian legislation does not expressly mandate the initiation of a domestic investigation upon receipt of information from foreign counterparts (from EU or non-EU states), Slovenian authorities have indicated that such investigations may be undertaken pursuant to the general provisions of the CPA, in particular Art. 148 and the subsequent provisions.

Criterion 40.20

(a) The ARO can spontaneously exchange information on proceeds of crime and other crime related property with foreign counterparts if considered relevant for the asset recovery tasks of the latter (Council Decision 2007/845/JHA, Art.4). Also, the judicial authority can forward information obtained during the performance of its tasks to the competent authorities of another EU MS without prior request (ACCMEU-1, Art. 52). Spontaneous exchange of information with foreign competent authorities from third countries can be done if so provided by an international agreement, and if such data may be useful for the implementation of a pre-trial criminal or criminal procedure in another country (CPA, Art. 516c).

(b) LEAs may initiate the tracing of assets on their own initiative and subsequently cooperate with foreign EU counterparts, upon receipt of intelligence or indicators that criminal property located in Slovenia may be relevant to an ongoing foreign investigation (Police Tasks and Powers Act, Art. 117.č and CPA, Art. 148). Concerning non-EU countries, LEAs advised that in practice the provisions of Art. 117(2) of the Police Tasks and Powers Act are also applicable with regard to the spontaneous identification and tracing of criminal property/ property of corresponding value.

Criterion 40.21

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 Arts. 514 and 515 CPA, 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.

Criterion 40.22

LEAs can form specialised investigative teams (SITs) and joint investigative teams (JITs) (CPA, Arts. 160a and 160b). 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.

Criterion 40.23

At the EU level, cooperation frameworks are designed to facilitate and enhance cooperation in cross-border investigations, such as the Anti-Money Laundering Operational Network (AMON) and the CARIN hosted by Europol. Slovenia is part of the above-mentioned networks and is also a member of Interpol and Eurojust, which support cross-border cooperation relevant to asset recovery.

Criterion 40.24

OMLP can exchange information indirectly with foreign non-counterparts and such exchange should be carried exclusively through the FIU of the foreign country. The purpose for which data is requested must be specified in OMLP's request (APMLTF-2, Arts. 123, 114(3)).

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.

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.

With regard to the supervisory authorities:

- BoS has the power to cooperate diagonally with non-counterpart authorities from EU as provided by Art. 16 BA.
- 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.

Slovenian legislation does not specifically ensure that the competent authority requesting information indirectly always makes it clear for what purpose and on whose behalf the request is made.

Weighting and Conclusion

Slovenian authorities can provide a very wide range of international cooperation to their foreign counterparts. The majority of criteria under R.40 are met, nevertheless some minor deficiencies are identified. **R.40 is rated LC.**

Annex B. TECHNICAL COMPLIANCE SHORTCOMINGS

Annex Table 1. Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks & applying a risk-based approach	PC	• There are no provisions for the dissemination directly to all relevant competent authorities, SRBs, FIs and DNFBPs (c.1.4). • There are no provisions for the assessment of PF risks, nor for the designation of an authority or mechanism to coordinate such assessments, to keep PF risk assessments up to date, or to ensure the appropriate dissemination of their results (c.1.5). • Slovenia does not have any risk mitigation provisions relating to PF risks (c.1.11). • Obligations to monitor the implementation of risk mitigation controls is limited to medium-sized and large OEs only. Furthermore, there are no obligations on any OEs to enhance controls if necessary (c.1.13(b)). Deficiencies under c.1.13(b) also have a bearing on c.1.14. • There are no provisions relating to PF risks imposed on FIs and DNFBPs (c.1.15).
2. National cooperation and coordination	PC	• Slovenia does not have any national policies regarding to PF (c.2.1). • There are no mechanisms to follow up or regularly review AML/CFT national policies (c.2.1). • There are limited formal inter-agency frameworks to specifically co-operate, co-ordinate an exchange information domestically, relating to national policies and strategies (c.2.2). • There are no frameworks, designated authority, or mechanism for the setting national policies and ensuring cooperation and coordination in respect to PF (c.2.3). • There are limitations in the mechanisms available to permit the effective operational co-operation, coordination and timely sharing of relevant information between competent authorities (c.2.4).
3. Money laundering offences	LC	• Slovenian legislation does not criminalise the act of ML in the form of simple possession and use of property (c.3.1). • There are some minor deficiencies in relation to the scope of application of certain ancillary offences (c.3.11).
4. Confiscation and provisional measures	PC	• There is no overarching policy which would target prioritisation of asset recovery issues in both domestic and international context (c.4.1(a)) • There is no comprehensive periodic review of the asset recovery regime (c.4.1(b)) • There is a lack of resources (c.4.1(c)) • FIU has no power to suspend a transaction in relation to predicate offence (c.4.3(a)) • No legal possibility to freeze and seize criminal property and property of corresponding value without a court order when it is necessary to act expeditiously (c.4.5)
5. Terrorist financing offence	LC	• TF offence does not include financing all of the offences listed in the Annex to the TF Convention (some minor offences are missing)
6. Targeted financial sanctions related to terrorism & TF	LC	• There is no EU procedure or requirements regarding the provision of identifying or supporting information with respect to requesting non-EU countries to give effect to EU designations. Information to support designation may be shared with non-EU members upon request provided EU member states agree. At the national level, there is no procedure in respect of requesting third countries to give effect to 1373 designations and regarding information to be provided for identification, as well as specific information to support the decision (c.6.2(e)). • Legal framework does not prescribe specific authorities or mechanisms to collect or solicit information to identify targets for designation (c.6.3(a)). • At the EU level, implementation of TFS, pursuant to UNSCRs 1267/1989 and 1988, does not occur “without delay.” For TFS under the UNSCR 1373 mechanism, these measures are implemented without delay, except in respect of EU internals (c.6.4). • At the EU level, for 1373 designations, there is no requirement to freeze assets of listed individuals that are EU internals. At the national level, there is no explicit requirement to freeze assets without delay and without prior notice. There are no additional freezing requirements set for natural and legal persons at the domestic level, hence UN designated EU internals will not be covered for the latter (c.6.5(a)). • At the EU level, freezing actions for UNSCRs 1267/1989 and 1988 do not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU

Recommendations	Rating	Factor(s) underlying the rating
		Best Practices on sanctions implementation. At the national level, measures in respect of UNSCRs 1267/1989 and 1988, as well as UNSCR 1373 designations do not appropriately extend to all funds and other assets (including jointly-owned assets) (c.6.5(b)). • Deficiencies in respect of freezing obligations noted under c.6.5(a) for EU internals apply also to criterion c.6.5(c). • At the EU level, there may be delays to updates via the newsletter service notably in case of designations on Fridays or over the weekend. At the national level, there is no domestic mechanisms in place to notify FIs and DNFBPs of UN and domestic designations immediately upon taking such action (c.6.5(d)). • At the EU level, requirement to report any information which would facilitate compliance with TFS obligations to their respective national competent authorities does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report “any information which would facilitate compliance” with the relevant Regulations. The scope gap in obligations in respect of 1373 designations (EU internals) also applies to this criterion (c.6.5(e)). At the national level, only FIs are required to report freezing of assets only under EU sanctions, to Bank of Slovenia (BoS). This falls short of requiring that all OEs report on frozen assets and actions taken on UN designated persons (c.6.5(e)). • At the national level, Slovenia does not to have publicly known procedures to unfreeze the funds of inadvertently affected persons (c.6.6(f)). • There are no domestic mechanisms in place to notify FIs and DNFBPs on UN and domestic de-listing and unfreezing immediately upon taking such an action. There is no specific guidance provided to FIs and DNFBPs on their obligations to respect a de-listing or unfreezing action (c.6.6(g)).
7. Targeted financial sanctions related to proliferation	LC	• At the EU level, implementation of TFS, pursuant to UNSCR 1718, does not occur “without delay.” This is due to the time taken to consult between EC departments and the translation of Commission or Council Implementing Regulations containing the designation into all official EU languages. At the national level, the regulatory framework and the identified gap as described under c.6.4 apply (c.7.1). • At the EU level, delays in implementation apply as described under c.7.1. At the national level, the regulatory framework and the identified gap as described under c.6.5(a) apply (c.7.2(a)). • At the EU level, freezing action for UNSCR 1718 does not explicitly cover jointly-owned assets, although this interpretation is taken in non-binding EU Best Practices on sanctions implementation (EC document 8519/18, para.34-35). While the definition does not explicitly cover funds or assets of persons acting on behalf or at the direction of a designated person or entity, this is largely captured by the coverage of funds ‘controlled’ by the designated person (Guidelines on implementation and evaluation of restrictive measures (sanctions) in the framework of the EU Common Foreign and Security Policy, Para 55b.). At the national level, the regulatory framework and the identified gap as described under c.6.5(b) apply (c.7.2(b)). • At the national level, the regulatory framework, set mechanisms and the identified gap as described under c.6.5(d) apply (c.7.2(d)). • At the EU level, the requirement to report any information which would facilitate compliance with TFS obligations does not explicitly extend to reporting attempted transactions, although this is covered by the requirement to report “any information which would facilitate compliance” with the relevant Regulations. At the national level, the same mechanism to report is used as for TF TFS (see c.6.5(e)) (c.7.2(e)). • At the national level, Slovenia does not to have publicly known procedures to unfreeze the funds of inadvertently affected persons (c.7.4(b)). • At the national level, the regulatory framework, set mechanisms and the identified gap as described under c.6.5(g) apply (c.7.4(d)). • At the EU level, regulations permit the addition of interests or other sums due on those accounts or payments due under contracts, agreements or obligations that arose prior to the date on which those accounts became subject to the provisions of this resolution, provided that these amounts are also subject to freezing measures. (EU Regulation 2017/1509, Art. 34(9)). At the national level, there are no measures to ensure that there are equivalent provisions in any UNSCR 1718 mechanisms implemented domestically (c.7.5(a)).
8. Non-profit organisations		• Slovenia did not identify the subset of NPOs that fall under the FATF definition for the further analysis of the TF risks (c.8.1(a)).

Recommendations	Rating	Factor(s) underlying the rating
		• The NRA identified a number of vulnerabilities that are pertinent to all NPOs in general but did not identify the risks of those individual NPOs and the nature of the TF risk posed on them (c.8.1(b)). • Besides applicable legislation, Slovenia has not indicated the existence of any focused, proportionate and risk-based measures to address the TF risks identified in the NPO sector, in line with the risk-based approach (c.8.1(c)). • There are no donor policies available in Slovenia (c.8.2 (a)). • The oversight and monitoring measures are rule-based, and hence not focused, proportionate or risk-based. Measures are applied regardless of TF risk to all NPOs operating in the country (c.8.3 (a) and (b)). • No relevant information about the oversight of NPOs since 2018 has been made available to the AT. Measures are applied regardless of TF risk to all NPOs operating in the country (c.8.4(a)). • The amounts of fines for both types of NPOs do not appear to be effective, or dissuasive. No information is provided on Humanitarian organisations (c.8.4 (b)). • There are no points of contact and procedures to respond to international requests for information regarding particular NPOs suspected of terrorist financing or involvement in other forms of terrorist support designated in Slovenia. However, those requests are handled within the framework of general international cooperation mechanisms (c.8.6).
9. Financial institution secrecy laws	LC	• There is no explicit exemptions from confidentiality provisions related to the exchange of information between all FIs where this is required under R.13, R.16 and R.17 (c.9.1).
10. Customer due diligence	LC	• In the case of an occasional transaction involving a wire transfer, CDD is to be carried out where the value of the wire transfer exceeds EUR 1 000 but not when the value of the wire transfer is EUR 1 000 (c.10.2(c)). • There is no clarity as to what is meant by 'suitable transparency of ownership' in the case of listed legal persons (c.10.5). • There is no obligation to review and update documents, information and data collected to establish the purpose and intended nature of a business relationship (c.10.7(b)). • There is no direct requirement to collect information on the powers that regulate and bind the legal person. Information on the names of the relevant persons having a senior management position in the legal person or arrangement are to be collected only where they are also vested with legal representation (c.10.9(b)). • Not all forms of control via other means may be captured (c.10.10(b)). • There is no obligation to identify and verify the identity of a beneficiary's BO, where this may be applicable, other than in situations where EDD is applicable (c.10.13) • There is no requirement to re-apply CDD measures (c.10.16). • There is no outright prohibition against applying SDD measures whenever specific higher risk scenarios apply (c.10.18). • There is no provision in the law that allows FIs not to pursue CDD requirements where they suspect ML or TF and reasonably believe that performing the CDD process will tip off the customer (c.10.20).
11. Record keeping	C	
12. Politically exposed persons	C	
13. Correspondent banking	LC	• There is no obligation for FIs to gather information on whether the respondent has been or is subject to ML/TF investigations or regulatory actions (c.13.1(a)).
14. Money or value transfer services	C	
15. New technologies	PC	• There is no requirement for FIs, other than retail banks, to carry out a risk assessment of developing technologies (c.15.1). • The assessment for virtual assets and for VASPs is not backed up by all relevant data and the risk ratings may therefore not reflect the actual risk (c.15.3(a)). • The actions to mitigate the abuse of VASPs and virtual assets rely on the coming into force of MiCAR only (c.15.3(b)).

Recommendations	Rating	Factor(s) underlying the rating
	LC	• Deficiencies identified under to c.1.12, c.1.13, c.1.14 and c.1.15 are applicable here too (c.15.3(c)). • There does not seem to be the possibility to remove a qualifying shareholder that is no longer deemed of sufficiently good repute to divest itself of its holding. It is unclear whether changes in the management body can take place once the notification requirement has been met or whether it is dependent on the SMA granting its approval thereto (c.15.4(b)). • There are shortcomings in the pecuniary penalties applied to unauthorised VASPs, and therefore on whether the sanctions applied in such cases are appropriate (c.15.5). • The shortcomings in the risk assessment and supervisory methodologies for the BoS and SMA identified under c 26.5 and c 26.6 are equally applicable to R.15 (c.15.6(a)). • There is no sector-wide guidance available for VASPs and feedback on the quality of STRs submitted by VASPs does not seem to be provided (c.15.7). • The deficiencies identified under c.35.1 and c. 35.2 are equally applicable here (c.15.8(a) and c.15.8(b)). • It is unclear whether the term funds, which is used to denote the threshold for the carrying out of CDD in the case of an occasional transaction, would also capture virtual assets (c.15.9(a)) • Deficiencies in respective criteria under R.6 and 7 find application here too (c.15.10).
16. Wire transfers	LC	• Information requirements do not apply to cross-border transfers equalling USD/EUR 1,000 (c.16.1, c.16.14). • There is no explicit obligation requiring PSPs to file a suspicious transaction report in all countries concerned by a suspicious wire transfer (c.16.17(b)).
17. Reliance on third parties	LC	• FIs are not required 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 (c.17.1(c)). • Third party reliance is permitted in case of EU Member States without having regard to the level of country risk (c.17.2). • There is no specific requirement for any higher country risk to be adequately mitigated by the group's AML/CFT policies (c.17.3(c)).
18. Internal controls and foreign branches and subsidiaries	LC	• The requirement to have policies and procedures for intra-group information exchange aimed at preventing money laundering and terrorist financing but does not contain an explicit reference to information exchange required for the ML/TF risk management purposes (c.18.2(a)). • There is no specific requirement on provision of information to or from the group-level compliance, audit and/or AML/CFT functions (c.18.2(b)). • No safeguards on the confidentiality and use of information exchanged is provided for other than data protection ones (c.18.2(c)). • There are no provisions regulating application of AML/CFT measures consistent with home country requirements for FIs that have branches or majority – owned subsidiaries in the EU Member States (c.18.3).
19. Higher-risk countries	LC	• Discretion is allowed to FIs as to whether to apply EDD measures to countries for which this is called for by the FATF (c.19.1). • Higher risk countries are limited to those on the EU's list of high risk third countries (c.19.2).
20. Reporting of suspicious transaction	LC	• Reporting of transactions which cannot be suspended have to be reported within a maximum of five business days and not promptly (c.20.1).
21. Tipping-off and confidentiality	LC	• Legislation is also silent on whether the exemption from professional secrecy and confidentiality obligations equally applies where FIs and their staff do not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred (c.21.1). • The obligation not to disclose the fact that an STR or related information is being filed is only valid for eight years (c.21.2).
22. DNFBPs: Customer due diligence	PC	• There is a scoping gap with regard to coverage of the legal advisors (R.22). • Real estate agents are not required to apply CDD requirements on both purchasers

Recommendations	Rating	Factor(s) underlying the rating
		and vendors (c.22.1(b)). • The definition of TCSP is not fully compliant with the FATF Standards (c.22.1(e)) • Deficiencies noted under R.10, R.15 and R.17 also apply in respect to DNFBPs (c.22.3-22.5)
23. DNFBPs: Other measures	LC	• There is a scoping gap with regard to coverage of the legal advisors (R.22). • Deficiencies noted under R.18, R.19, R.20, and R.21 also apply in respect to DNFBPs (c.23.1-23.4)
24. Transparency and beneficial ownership of legal persons	PC	• No ML/TF risk assessment has been carried out on foreign legal persons to take into account the ML/TF risk they may pose to Slovenia. BO information is only available through reporting entities and, where a legal person has a branch in Slovenia, through the RBO (c.24.1(d)). • The current NRA (a) does no consider exhaustively the ML/TF risks posed by legal persons established under the laws of Slovenia; and (b) does not contain any information on or assessment of the ML/TF risks posed by the different types of foreign-created legal persons that have links with the country (c.24.3). • The obligation on legal persons to retain information does not extend to the statutory documents of the company nor to all directors unless they also have legal representation (c.24.5(a)). • Companies are not obliged to maintain registers on shareholders/members/partners (c.24.5(b)-(c)). • While companies are obliged to ensure that the information is kept accurate, there is no reference as to how this is to be done. Companies have to update the information at every data modification. However, no timeframe is set for companies within which the information is to be updated (24.6(a)). • Information on BOs that are foreign residents is not verified by authorities when it is registered in the BO Register. There is no mechanism to ensure that all legal persons established in Slovenia actually provide information on their BOs at incorporation or on an on-going basis (c.24.8). • Only branches of foreign legal persons have to disclose beneficial ownership information to the BO Register. BO information may be available through reporting entities but this is dependent on foreign legal persons having a relationship therewith (c.24.10). • Pecuniary penalties imposed for breaches of obligations relative to basic and BO information are not considered as proportionate, dissuasive and effective (c.24.14). • In the case of tax authorities, the exchange of information can only take place within the context of a treaty or EU legislation (c.24.15(a)). • There is no obligation to monitor the quality of basic and/or BO information received in response to a request for information (c.24.15 (e)). • Reliance on reporting entities to provide BO information does not result in BO information being readily available (c.24.15(f)). • There is limited publicly available information on how to contact agencies responsible for responding to all international requests for beneficial ownership information (c.24.15(g)).
25. Transparency and beneficial ownership of legal arrangements	PC	• No risk assessment of trusts or similar legal arrangements managed or administered from Slovenia has been undertaken (c.25.1). • The NRA does not assess the ML/TF risks associated with trusts or similar legal arrangements which are either (i) administered from within Slovenia or the trustee resides in Slovenia; or (ii) are governed by foreign law but have sufficient links to Slovenia (c.25.3(b) and (c)). • Objects of power who are identified but in whose favour the trustee has not yet exercised its discretion are not covered (c.25.4(a)). • There is no obligation to determine the BO of any party to a trust that happens to be a legal person or a legal arrangement (c.25.4(b)). • No reference is made to the trustee having to hold basic information on other regulated agents of, and service providers to, the trust and similar legal arrangement, including but not limited to investment advisors or managers, accountants and tax advisors (c25.4(c)).

Recommendations	Rating	Factor(s) underlying the rating
		• No indication was provided as to whether there are disclosure obligations that cater for the disclosure of information, other than BO information, held by the trustee or anyone holding a similar position within a legal arrangement (c.25.7 (b)-(c)). • Information on BOs that are foreign residents is not verified by authorities when it is registered in the BO Register. There is no mechanism to ensure that all legal arrangements established in Slovenia actually provide information on their BOs at establishment or on an on-going basis (c.25.8 and c.25.9 (a)). • It is unclear to what extent the OEs are a source of BO information with respect to legal arrangements when carrying out services triggering AML/CFT obligations (c.25.9(c)). • Limitations to the BO definition under c.25.4(a) have a bearing on c.25.10(a). • Pecuniary penalties imposed for breaches of obligations relative to basic and BO information are not considered as proportionate, dissuasive and effective (c.25.11(b)(c)). • In the case of tax authorities, the exchange of information can only take place within the context of a treaty or EU legislation (c.25.12(a)). • There is limited publicly available information on how to contact agencies responsible for responding to all international requests for beneficial ownership information. Reliance on reporting entities to provide BO information does not result in BO information being readily available (c.25.12(e)).
26. Regulation and supervision of financial institutions	LC	• There are a series of shortcomings that limit the authorities' ability to ensure that qualifying shareholders and members of the management bodies are fit and proper (c.26.3). • Not all supervisory authorities take into account the group aspect in determining the frequency and intensity of on-site and off-site AML/CFT supervision (c.26.4).
27. Powers of supervisors	LC	• It is not clear from where the powers of MIRS to carry out any form of supervisory engagements derive (c.27.2). • It is not clear from MIRS derives its powers to compel the product of information and documents for the purposes of its supervisory activity (c.27.3). • The sanctions that supervisory authorities can impose are not aligned with R. 35 (c.27.4).
28. Regulation and supervision of DNFBPs	PC	• There is a scoping gap with regard to coverage of the legal advisors (R.28) • Slovenia does not have legal provisions to prevent criminal associates from holding a significant or controlling interest in a casino (c.28.1(b)). • There is no designated supervisory body or SRB to regulate legal professionals that are not registered with the BAS, however can still carry out activities that fall within the FATF Standards (c.28.2). • There are no provisions to prevent criminals from owning or controlling, or holding a management function within the following: TCSPs, DPMS, tax advisors or accountants. Furthermore, there are no legal provisions to prevent criminal associates from holding a significant or controlling interest in a DNFBP. (c.28.4(b)). • Deficiencies noted under R.35 also apply in respect to DNFBPs (c.28.4(c)) • There are no provisions for supervision to be conducted on a risk-sensitive basis taking into account the DNFBPs risk profile or characteristics, in particular their diversity and number (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	• There is high evidentiary threshold necessary to obtain banking information (c.31.1(a)) • The provisions regulating controlled delivery are not sufficiently wide in scope (c.31.3)
32. Cash couriers	LC	• There still is requirement for physical cross-border movement of cash by mail and cargo within the EU (c.32.1) • No provisions for oral declarations have been implemented (c.32.2)

Recommendations	Rating	Factor(s) underlying the rating
33. Statistics	LC	• The legislation does not explicitly impose the relevant authority to keep statistics on MLA
34. Guidance and feedback	LC	• No information was provided by the FARS, SBA, CNS and PCGRM regarding feedback (c.34.1).
35. Sanctions	PC	• The absence of clear sanctioning policies and weighting criteria undermines consistency and proportionality in enforcement outcomes. In addition, the legal thresholds for imposing higher administrative penalties are narrowly defined, which may constrain authorities' ability to apply effective and dissuasive sanctions in serious AML/CFT breaches (c.35.1). • The need to align minor offences under the APMLTF-2 with the Minor Offences Act entails that no action can take place within 2 years from when the breach is detected. Furthermore, the automatic application of a 50% discount for early payment of fines without consideration by the respective supervisory authority or SRB, limits the effectiveness of the sanctions regime (c.35.1). • The provisions to permanently or temporary ban individuals is limited to Directors and does not apply to senior management or other individuals conducting key functions (c.35.2).
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
37. Mutual legal assistance	LC	• Minor deficiencies observed in relation to R. 3 and 5 may restrict the range of mutual assistance in cases where dual criminality is required • No case management systems for monitoring direct communications with EU member states
38. Mutual legal assistance: freezing and confiscation	LC	• There is a minor gap – threshold of EUR 50 000 for providing assistance in instances when confiscation order of a foreign state was brought in civil proceeding (c.38.1) • Deficiencies observed in relation to R.4 restrict the execution of freezing order if it was not ordered by court (c.38.2) • There is no domestic legal framework covering the deduction or share of substantial extraordinary costs incurred with the enforcement of a freezing/seizing/confiscation order of non-EU countries (c.38.7 (b))
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 AML/CFT law and the sectoral legislation (BA, FIMA and IA) do not provide for the use of secure gateways for the exchange of information at international level (c.40.1) • Police, ISA and SMA do not have a standard procedure for giving feedback to a foreign authority (c.40.4) • There is minor shortcoming in the legal possibility to exchange all obtainable information with foreign counterparts (c.40.8) • BoS and ISA as supervisors have full powers to facilitate group supervision only with regard to EU countries (c.40.16)

Note:

Glossary of Acronyms

	DEFINITION
AA	Associations Act
AML/CFT/CPF	Anti-Money Laundering, Combating the Financing of Terrorism and Combatting the Financing of Proliferation of Weapons of Mass Destruction
ACCMEU	Act on Cooperation in Criminal Matters with the EU Member States
ACIOP	Confiscation of Assets of Illicit Origin Act
AJPES	Agency of the Republic of Slovenia for Public Legal Records and Related Services
AMON	Anti-Money Laundering Operational Network
AMO	Asset management office
APOA	Agency for Public Oversight of Auditing
APMLTF-2	Act on the Prevention of Money Laundering and Terrorism Financing
ARM	Act on Restrictive Measures
ARO	Asset recovery office
BA	Banking Act
BAA	Bar Association Act
BESA	Book Entry Securities Act
BNIs	Bearer negotiable instruments
BOs	Beneficial owners
BoS	Bank of Slovenia
BRA	Business Register Act
CA	Companies Act
CARIN	Camden Asset Recovery Inter-Agency Network
CC	Criminal Code
CDD	Customer Due Diligence
CNS	Chamber of Notaries of Slovenia
COMET	Council's Working Party on the Application of Specific Measures to Combat Terrorism
CPA	Criminal Procedure Act
CRA	Court Register Act
CSCC	Central Securities Clearing Corporation
DLT	Distributed ledger technology
EEA	European Economic Area
EAW	European Arret Warrant
EBA	European Banking Authority
EC	European Commission

EDD	Enhanced due diligence
EES	Entry/Exit System
EFO	European Freezing Order
EIC	Expert Information Centre of the SPO
EIO	European Investigative order
EJN	European Judicial Network
EMIs	Electronic money institutions
EPPO	European Public Prosecutor's Office
ESMA	European Securities and Markets Authority
ETIAS	European Travel Information and Authorisation System
EU	European Union
EURODAC	European Asylum Dactyloscopy Database
EUROJUST	European Union Agency for Criminal Justice Cooperation
EUROPOL	European Union Agency for Law Enforcement Cooperation,
FA	Foundation Act
FAA	Foreign Affairs Act
FARS	Financial Administration of the Republic of Slovenia
FCMLS	Financial Crime and Money Laundering Section
FI	Financial institution
FIMA	Financial Instruments Market Act
FIU	Financial intelligence unit
FUR	Follow-up report
FRM	Financial restrictive measures
HKOM	Central Public Administration Communication Network
HR	High Representative for Foreign Affairs and Security Policy
IA	Insurance Act
IOSCO	International Organization of Securities Commissions
ISA	Insurance Supervisory Agency
ISUPPD	the OMLP's database
IWG	Interministerial Working Group
JIT	Joint investigation team
LEA	Law enforcement authority
LLPA	Liability of Legal Persons for Criminal Offences Act
MFEA	Ministry of Foreign and European Affairs
MIRS	Market Inspectorate of the Republic of Slovenia
ML	Money laundering
MLA	Mutual legal assistance
MOA	Minor Offences Act
MoF	Ministry of Finance
MoJ	Ministry of Justice
MOU	Memorandum of understanding
MVTS	Money or Value Transfer Services
NPU	National Bureau of Investigation
NGOs	Non-governmental organization
NPO	Non-profit organisation
NRA	National risk assessment
OEs	Obliged entity
OLAF	European Anti-Fraud Office
OMLP	Office for Money Laundering Prevention of the Republic of Slovenia

OPSI	Slovenian Open Data Portal
PCGRM	Permanent Coordination Group on Restrictive Measures
PEP	Politically Exposed Person
PF	Proliferation Financing
PI	Payment institution
PSPs	Payment service providers
PSSIEMPSA	Payment Services, Services of Issuing Electronic Money and Payment Systems Act
RBO	Register of Beneficial Ownership
RoP	Rules of Procedure
SBA	Slovenian Bar Association
SBR	Slovenia Business Register
SDD	Simplified due diligence
SIS	Schengen Information System
SITs	Specialised investigative teams
SMA	Securities Market Agency
SOVA	Slovenian Intelligence and Security Agency
SPO	State Prosecutor's Office
SPOT	State Portal for Business Registry
SRB	Self-Regulatory Body
SSPO	Specialised State Prosecutor’s Office
STRs	Suspicious transaction reports
TCSPs	Trust or Company Service Providers
TF	Terrorist financing
TFS	Targeted financial sanctions
UCITS	Undertakings for Collective Investment in Transferable Securities
UNCAC	UN Convention against Corruption
UNSC	United Nations Security Council
UNSCR	United Nations Security Council resolution
VAs	Virtual assets
VASPs	Virtual asset service providers
WP	Working party

www.coe.int/MONEYVAL

May 2026

Anti-money laundering and counter-terrorist financing measures -
Slovenia
Sixth Round Mutual Evaluation Report

This report provides a summary of AML/CFT measures in place in Slovenia as at the date of the on-site visit (10.10.2025). 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.