Mutual Evaluation Report of the Republic of Uzbekistan

2022

ЕВРАЗИЙСКАЯ ГРУППА
по противодействию легализации преступных доходов
и финансированию терроризма

EURASIAN GROUP
on combating money laundering
and financing of terrorism

Contents

EXECUTIVE SUMMARY

Key Findings

1. This Report summarizes the AML/CFT/CPF measures in place in the Republic of Uzbekistan as at the date of the on-site visit of the EAG assessment team (June 14 – July 2, 2021). It analyzes the level of compliance with the FATF Recommendations and the level of effectiveness of the AML/CFT system of the Republic of Uzbekistan, and recommends how the national AML/CFT system could be strengthened and how the AML/CFT measures taken by the competent authorities could be enhanced.

1. The Republic of Uzbekistan is making significant efforts to identify, understand and assess its ML/TF risks and develop measures to mitigate them. The 2019 NRA findings related to ML/TF risks seem reasonable and well substantiated. However, there is the need for additional analysis of certain categories of ML/TF threats so as to more accurately reflect the country's profile. The aims and objectives of competent authorities are largely consistent with national ML/TF risks. The country largely ensures that the findings and conclusions of the NRA are communicated to the private sector.
2. A high level of inter-agency cooperation characterizes the AML/CFT/CPF system in Uzbekistan to obtain financial intelligence. All LEAs have access to a wide range of financial information which may be obtained either independently or by contacting the FIU. All financial and non-financial information received by the DCEC is analysed in a risk-based approach and transmitted to the competent authorities as quickly as possible.
3. The identified and investigated ML typologies, schemes and techniques are in common consistent with the national threats and risks and the national AML policies. Most ML cases identified in Uzbekistan are related to self-laundering and do not involve complex ML schemes. The LEAs are focused on priority solving predicate crimes, the criminal prosecution agencies lacked common practice of (parallel) financial investigations until 2021.
4. Sanctions for ML offences provided for in the legislation are dissuasive, but not proportionate and for TF are dissuasive and proportionate. Sanctions are not imposed on legal entities involved in ML/TF.
5. The priority application of confiscation is compensation for material damage (restitution to victims). Confiscation is based solely on criminal procedural mechanisms. Non-conviction based confiscation is applied in cases limited by the country's law.
6. Competent authorities are well acquainted with current TF risks and adequately response to emerging challenges. In whole, investigations conducted by LEAs are in line with the Uzbekistan's risk profile. LEAs pay strong attention to outside TF risks, however, the risk of domestic financing seems to be underestimated to a small extent.
7. Uzbekistan seeks to deprive terrorists, terrorist organisations and individuals who finance terrorist activities of their assets and the means to commit crimes through various methods. Recently (for 2 years), there has been a coherent system of implementation and application of the TFS, which allows applying the TFS regime without delay. The lack of cases where the Republic of Uzbekistan has submitted proposals for inclusion on the UNSC sanctions lists may be a disadvantage, given a large number of individuals on the national section of the List.
8. There is a significant level of proportionate measures applied to vulnerable NPOs in the country, both general and targeted. Specific controls are used under the RBA. Applying these measures in combination addresses the existing risk of NPOs being used for TF purposes.
9. The Republic of Uzbekistan has a uniform legal framework as to CPF and CFT. Competent authorities and the private sector have made practical steps towards the timely inclusion of those related to the PF into the corresponding List and are taking measures as to freezing.

10. FIs and DNFBPs demonstrated an understanding of ML/TF risks based on the NRA findings and training activities conducted by the competent authorities. All FIs and DNFBPs apply internal control procedures in accordance with the established ICRs, which are binding on the organisation.
11. The FIs supervision is well established, for the DNFBP sector is insufficient. Sanctions for violations of AML/CFT requirements are actively applied only by the CB to banks and NBCI and by commodity exchanges to their members; in other sectors, sanctions are spotty or not applied.
12. Legal persons could be misused for the purposes of ML, acting primarily as a tool and facilitator for cashing-out funds. Conditions have been established to mitigate the misuse of legal persons with a special attention given to ensure the accuracy of basic information and BO data. The sector of professional accounting and legal service providers is not fully explored. Sanctions for non-compliance with requirements to provide information on legal persons and BO are not sufficient. There is no regulation of registering body's obligation to carry out verification of information provided during state registration.
13. The republic provides legal assistance in a constructive and timely manner. LEAs use the MLA mechanism to search for assets, but priority is given to other forms of cooperation. The state authorities effectively cooperate in the extradition of criminals. Information exchange through the FIU is carried out perpetually. International collaboration on issues of supervision is limited.
14. All competent authorities are able to receive and provide beneficial ownership information via the MLA channels, but there is no common understanding of the sequence of actions to collect appropriate data in such cases.

Risks and General Situation

2. The Republic of Uzbekistan has made significant efforts to identify, understand and assess its ML/TF risks and develop measures to mitigate them. This work has intensified significantly starting in 2017.
3. In 2019, the country conducted an NRA, report approved by the decision of the IAC of 30.12.2019. There is a substantial overall level of understanding of national ML/TF risks based on the findings of the conducted NRA.
4. The ML risks associated with corruption and bribery, tax and customs offences, illicit drug trafficking, organized crime, fraud and violation of the trade and service provision regulations are assessed as very high. At the medium level is the risk of ML from human trafficking, unlicensed activities, illegal trade in medicines, smuggling, acquisition and sale of criminal assets, extortion, illegal production of stamps, documents, seals, illicit production of alcohol and tobacco products, environmental crimes.
5. Relevant are schemes related to illegal transit (including cross-border) and money laundering. Considering contextual factors specific to the Republic of Uzbekistan and legislative regulation (see R.15), the risks of involvement of VASP in ML schemes were assessed as low; however, there is a high probability of using VA to commit predicate offences.
6. The main identified TF typologies involve movement of funds through intermediaries (cash couriers, hawala), transfer of funds through the payment systems, online transfer of funds with the use of bank cards, misuse of money remittance systems and purchase of airline tickets and other travel documents for foreign terrorist fighters (FTFs). The country is largely aware of the risks of TF. Still, more attention is needed to identify the threats and instances of TF within the country and strengthen outreach to the private sector to prevent possible cases of TF.
7. Public foundations and religious organisations are recognised in the 2020 NRA SRA as vulnerable to being used for FT purposes.
8. The findings of the NRA are reasonable; however, the analysis has provided evidence that the degree of threat of frauds and robberies/thefts is underestimated.

Overall Level of Effectiveness and Technical Compliance

9. Uzbekistan has achieved a significant progress in building the effective AML/CFT/CPF system. In the course of the reforms initiated in Uzbekistan, the AML/CFT/CPF legislation has been substantially modified, the TFS regime has been enhanced, the FI and DNFBP compliance mechanisms have been improved and a significant number of automated processing systems have been adopted, which ensures the effective operation of all AML/CTF system stakeholders.

10. Uzbekistan has made notable improvements in its overall level of technical compliance with the FATF Recommendations, although some weaknesses remain. The Uzbek legislation is compliant or largely compliant with the most relevant requirements of the FATF Recommendations. Since the previous mutual evaluation (conducted in 2010), most laws, regulations and other legislative acts pertaining to the assessed issued have been substantially amended and modified. Legislation governing the powers of the LEAs and the competence of the FIU is in line with AML/CFT/CPF standards. ML and TF offences are criminalised, and asset freezing and confiscation mechanisms are in place but need to be improved. The powers of competent authorities to coordinate and cooperate on AML/CFT/CPF issues at both national and international levels are regulated. The CDD, record keeping and suspicious transaction reporting obligations of the reporting entities are defined in the legislation.

11. Uzbekistan has demonstrated a substantial level of effectiveness in developing and pursuing the national AML/CFT/CPF policies and understanding of the existing ML/TF risks. A substantial level of effectiveness has also been demonstrated in terms of the work conducted by the FIU and the use of financial intelligence for identifying, investigating, disrupting and prosecuting ML/TF and associated predicate offences. The country has built an effective TF system based on preventive measures and without delay application of the TFS mechanism. Some progress has been made in applying proportionate and targeted measures to the activities of NPOs vulnerable to TF.

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

12. In the Republic of Uzbekistan, the FIU carries out the coordination of ML/TF risk assessment measures. The Interagency AML/CFT/CPF Commission (IAC) as a coordinating body for interagency cooperation on AML/CFT/CPF issues has been established and operates out of the deputy heads of ministries and agencies (23 members of the commission in total). The Chairman of the IAC is the Deputy Prosecutor General of the Republic of Uzbekistan.

13. Uzbekistan conducted the NRA in 2019. The unclassified NRA findings were published for general public on the FIU website and were also posted on the websites of the supervisory authorities and communicated to financial institutions and DNFBPs. The full version of the NRA report was disseminated to the ministries, government agencies and all supervisory authorities via the secure communication channels.

14. The FIU coordinated the NRA; its analyses were essential for this work. The LEAs provided statistical data and other information. The supervisory authorities disseminated the relevant questionnaires to their respective supervised entities and actively engaged with the private sector. The final NRA report reflects the concerted position of all competent ministries and government agencies.

15. The competent authorities have demonstrated a substantial overall level of understanding of the national ML/TF risks and good enough approaches to the development of the risk assessment methodology.

16. The private sector entities are aware of the NRA findings and the identified ML/TF risks, however, the degree of understanding of risks varies depending on the size and development of the sector.

17. The list of response measures have been developed for mitigating the identified ML/TF risks. The set out measures are ranked in order of priority of their implementation depending on level of the relevant

risks. The highest priority is given to adoption of the National AML/CFT/CPF Strategy[1] as well as to combating corruption, disruption of illegal payment systems, strengthening of fight against tax and customs crimes and improvement of transparency of FI and DNFBP customers and transactions.

18. Experts identified certain shortcomings in the ML/TF risk analysis (ML threat assessment and insufficient assessment of NPO-related risks) and vulnerabilities for which mitigation measures have not been taken (definition of the concept of national PEPs).

19. The competent authorities, based on the results of the NRA, adjusted their programmes and strategies to minimise the identified risks in accordance with their mandate. Many LEAs restructured their units and optimised their staffing levels to improve their priority areas in line with the identified risks and to optimise the allocation of resources. All supervisors updated the ICRs for the relevant FIs and DNFBPs regarding the ML/TF risks reflected and the preventive measures aimed at mitigating them.

20. Public authorities use various forms of dissemination and communication of NRA findings to the private sector. The findings of the NRA are used by FIs and DNFBPs to justify the need for enhanced measures where there is a higher risk situation, based on geographic characteristics, in the customer profile and to determine the risk profile of the transactions being conducted.

Financial Intelligence, Money Laundering and Confiscation (Chapter 3 – IO.6-8, R.3, R.4, R.29-32)

21. Uzbekistan has established the Department on Combating Economic Crime under the General Prosecutor's Office (DCEC) – a special LEA responsible for gathering criminal intelligence and conducting investigations and inquiries into economic and corruption-related offences as well as into ML/TF/PF offences, which is at the same time the national financial intelligence unit.

22. The DCEC is the central body that collects and analyzes STRs and other information received from financial institutions and DNFBPs and also plays the leading role in process of financial investigations. The bulk of information is received by the DCEC from credit institutions. Only few STRs and other reports are filed by the securities market participants and the exchange members. Almost no reports are provided by other financial institutions, and a few STRs have been received from the DNFBP sectors.

23. The LEAs have access to a wide range of financial intelligence for investigating predicate offences and ML/TF. The powers vested in the DCEC allow it to collect and disseminate any information, including data constituting bank and other secrets protected by the law. The LEAs regularly initiate criminal proceedings using the disseminations received from the DCEC.

24. All LEAs are aware of the FIU capability to promptly obtain meaningful information from abroad and use it in practice. Uzbekistan has arranged a sound interagency cooperation mechanism.

25. Uzbekistan has sufficient legislative and institutional framework for identifying and investigating ML cases. The appropriate measures are in place to ensure confidentiality and security of collected criminal intelligence and other information constituting commercial, bank and other secrets protected by the law.

26. In the process of criminal intelligence and detective activities (OIA), ML offences may be identified and disrupted by any agency involved in criminal intelligence gathering. Most ML cases were identified in the process of criminal investigations into predicate offences, which may implicitly indicate that the LEAs are primarily focused on detection of predicate offences.

27. Most ML cases identified in Uzbekistan are related to self-laundering, and only few instances of third-party ML and professional ML have been detected. The share of the identified ML offences is relatively small compared to the total number of committed predicate offences.

[1] The Strategy was adopted by Presidential Decree No.UP-6252 on Adoption of the Uzbek National Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing System Development Strategy dated June 28, 2021

28. ML prosecution generally takes place as part of prosecution for a predicate offence, or after a person is convicted for a predicate offence or after the proceedings on the primary offence are terminated for reasons other than exoneration. This is facilitated by the fact that the investigation of ML for a general rule is the competence of the MIA. Making the ML offence solely the responsibility of the MIA may lead to a lack of interest on the part of the bodies in charge of the OIA in detecting such crimes, as in fact, detecting ML offences is not one of their main responsibilities.
29. The parallel financial investigation procedure is governed by the joint regulations of the LEAs. Financial investigations are conducted through criminal intelligence gathering and detective operations (including joint investigations and proceedings), financial analysis, collection of information using different information resources (including the interagency electronic information exchange system), and use of various publicly accessible and internal information sources. However, understanding the purposes, methods, and sources of information in financial (parallel) investigations varies between agencies
30. The courts hear all types of ML-related criminal cases, irrespective of ML types (self-laundering, third-party ML, etc.) and categories of underlying predicate offences. Since the preliminary investigation and court trial functions are separated from each other and are discharged independently by different authorities, the judicial system cannot influence decision-making relating to the institution of ML criminal cases or referring such cases to courts.
31. Although legal entities may be held liable and be liquidated under the applicable civil law, no sanctions are imposed on legal entities for ML. The criminal sanctions against natural persons provided for in article 243 of the Criminal Code (CC) are dissuasive, but not proportionate.
32. Compensation of the inflicted damages and losses (restitution to victims) is one of the primary objectives of the national anti-crime policy. Criminal proceeds are confiscated when it is impossible to identify a person who suffered losses, or when assets may not be returned to a victim, or when the value of assets exceeds the inflicted losses.
33. Confiscation is based solely on the criminal procedure mechanisms, and property may be confiscated only subject to initiated criminal prosecution. The use of non-conviction based confiscation is limited.

Terrorist and Proliferation Financing (Chapter 4 – IO.9-11, R.5-8)

34. The authorities are well aware of the threat of international terrorism and its risks. The measures taken by the authorities are generally consistent with the overall TF risk profile of the country. However, LEAs pay serious attention to TF threats outside the country, but the risk of domestic financing appears to be underestimated to a small extent.
35. The anti-terrorist activities, including the CFT efforts, are coordinated through various interagency mechanisms, some of which are non-public. The IAC coordinates this work at the strategic level.
36. The competent authorities have demonstrated adequate understanding of TF risks. However, close vicinity of Uzbekistan to the zones with increased terrorist activities, including the immediate border with Afghanistan, along with low income of unqualified working-age population, maintain TF risks at high enough level.
37. The national list of terrorist organizations has not been updated since its adoption by the Supreme Court (SC) in 2016. The national section of the List of terrorist organisations is linked to the possibility of prosecution for TF, and this may lead to a loss of focus by LEAs on detection of the funding of some ITO, i.e. the detection and investigation of TF associated with organisations, not on the national List.
38. The LEAs have special units responsible for combating terrorism, including terrorist financing. Almost in all cases, the LEAs investigate TF cases and successfully press charges against suspects and bring such cases to court. The TF sanctions imposed by courts on guilty persons seem to be proportionate and dissuasive. Sanctions against legal entities are not applied.

39. Uzbekistan has recently (for 2 years) had a coherent system for the implementation and application of the TFS regime, which allows for the application of the TFS regime without delay. In previous years, the system did not fully enforce that principle.
40. Most reporting entities understand their obligations related to application of targeted financial sanctions.
41. The lack of cases where the Republic of Uzbekistan has submitted proposals for inclusion on the UNSC sanctions lists may be a weakness, given the large number of individuals on the national section of the List.
42. There is a significant level of proportionate application of both general and targeted measures to the vulnerable NPOs in the country. In doing so, specific control measures are applied in accordance with the RBA, while general ones are applied within a unified regulatory and supervisory framework. The application of these measures in combination mitigates the existing risk of NPOs being used for TF purposes, which is proved by the absence of such instances despite the high level of TF risk identified in the NRA.
43. NPOs have demonstrated a sufficient level of understanding of vulnerability of their misuse for TF purposes. No instances of misuse of NPOs for TF purposes have been recorded in the assessed period.
44. Uzbekistan has established a comprehensive legal framework and designated the competent agencies responsible for responding to and combating TF and PF. These agencies perform monitoring and, to a large extent, ensure compliance by reporting entities with the obligations related to the implementation of targeted financial sanctions for PF. Besides that, Uzbekistan has established an effective customs and export control system, one of the objectives of which is to monitor the movement of dual-use goods.

Preventive Measures (Chapter 5 – IO.4, R.9-23)

45. FIs and DNFBPs have demonstrated a good understanding of ML/TF risks and risk management measures based on NRA findings and training delivered by competent authorities. Financial institutions (FIs) understand their AML/CFT obligations, with banks, payment institutions sector, NBCIs, leasing companies, demonstrating the best understanding of such obligations among FIs. DNFBPs largely understand their AML/CFT obligations given the specific features of their respective sectors. The most complete understanding of such obligations and ML/TF risks was demonstrated by lawyers, notaries, lottery organisers and auditors.
46. FIs apply regular and enhanced CDD measures based on the established criteria, monitor transactions of their customers, and keep the obtained data. Enhanced CDD measures apply to foreign and international PEPs. In contrast, measures do not apply to domestic PEPs due to the lack of such a requirement in the legislation, which negatively affects the AML/CFT system.
47. FIs supervised by the CB use the special software that automatically screens customers against the lists of designated persons. Insofar as the banking sector is concerned, there have been instances when funds were frozen because data on customers matched the ID data of the designated persons included in the lists. Banks, exchange members, payment institutions, professional securities market participants and NBCIs diligently comply with the STR filing obligation in accordance with the established suspicious criteria.
48. All DNFBPs apply measures to mitigate ML/TF risks when on-boarding new customers and screen them against the lists of designated persons.
49. Although all DNFBPs understand their obligations pertaining to the provision of information to the designated government agency, not all DNFBP sector entities file STRs and other meaningful information with the DCEC. The exception is the notary sector, which sent 4 STRs for the entire period under review. At the same time, the DPMS sector demonstrated the weakest understanding of this responsibility.

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

50. Uzbekistan has established a regime for supervising activities of financial institutions and DNFBPs. The supervisory authorities as well as the leasing associations (SRO, in addition to the Ministry of Finance, exercises supervision) and commodity exchanges (non-public body with responsibilities aimed at ensuring compliance by exchange members) have a good understanding of ML/TF risks in the supervised sectors, develop risk mitigation measures and communicate them to the private sector.
51. The established requirements for licensing or special procedure of registration with the supervisory authorities for most FIs sufficiently prevent individuals who have been previously convicted for certain categories of criminal offences from holding management functions in financial institutions. Due to the high diversity and heterogeneity of DNFBP sectors, the effectiveness of measures taken for preventing criminals and their associates from being the owners or managers of companies varies significantly from sector to sector. There is a high level of efficiency in the lawyers and notaries sector and a lack of efficiency in other sectors, especially in the real estate and DPMS sectors, where such restrictions are almost completely absent.
52. The beneficial owner (BO) identification requirements are established for banks through a ban on the registration of entities with complex ownership structures. There are no BO identification mechanisms in place for other FIs, and no requirements for verifying the business reputation of beneficial owners and persons affiliated with them are established for all FIs.
53. The supervisory authorities effectively carry out preventive measures to detect unlicensed activities in the payment institutions, VASPs, and securities sectors.
54. Sanctions for breaches of the AML/CFT requirements are extensively applied by the CB and commodity exchanges and seem proportionate and dissuasive. The AML/CFT sanctions applicable against DNFBPs have no dissuasive effect and no impact on compliance with the mandatory AML/CFT requirements due to the lack of practical application.
55. Supervisors actively engage with the private sector entities with the view to assisting them in understanding ML/TF risks and raising overall awareness of their supervised entities by way of arranging various AML/CFT training events.

Transparency of Legal Persons and Arrangements (Chapter 7 – IO.5, R.24-25)

56. Information on the creation and categories of legal persons, as well as their Registry is publicly available. Legal persons inform state authorities about changes in charter documents, founders and composition of their shares, beneficiaries, as well as all other changes usually within 10 days.
57. Legal arrangements, in the sense how this term is used in the FATF Recommendations, cannot be created in Uzbekistan. The legislation assumes a relationship between foreign trusts and residents to receive income for the benefit of a settlor. At the time of the on-site mission, no relations with foreign trusts were recorded by residents.
58. The competent authorities demonstrated a good understanding of the vulnerabilities of legal persons. However, the extent of this understanding varies among government agencies. The assessment of vulnerabilities of legal persons was conducted in the framework of the NRA. There were no cases known (or identified) of misusing legal persons for TF purposes at the time of the on-site mission. LLCs are most often used for illegal purposes, including ML. Independent accountants and lawyers are not involved in the national AML/CFT system. The sector of professional accounting and legal service providers is not fully explored.
59. The country has created conditions to mitigate the misuse of legal persons, special attention is paid to ensuring the accuracy of basic information and BO. Legal persons carry out settlements in non-cash form. The activities of legal persons are inspected and if violations are detected sanctions are applied in respect to officials in the form of financial penalties. Legal acts are being modernized.

When residents apply to FIs and DNFBPs to conduct financial transactions with a party of a foreign trust, CDD measures are applied. LEAs have been successful in enforcing laws and preventing the misuse of legal persons. The measures taken generally correlate with the vulnerabilities of legal persons identified by the NRA.

60. The main source of basic information and BO with regard to all categories of legal persons created in the country is the SSRBE. There are additional sources of information, including data collected by FIs and DNFBPs. Competent authorities have unconditional access to these sources of information on legal persons and positively assess the quality of information. There are no sanctions in Uzbekistan for providing inaccurate or unreliable information at the registration. Sanctions are applied for failure to provide data in case of changes. Sanctions for non-compliance with the requirements for keeping and providing information on legal persons and BO, as well as limited measures against some DNFBPs for failure to collect the said information, are considered by assessors as not sufficient.

International Cooperation (Chapter 8 – IO.2, R.36-40)

61. Uzbekistan has adopted a sufficient legislative and regulatory framework for providing mutual legal assistance (MLA), including in extradition-related matters, and other forms of international cooperation. There are several central bodies (Supreme Court, Ministry of Internal Affairs, State Security Service, General Prosecutor's Office), which may act directly in accordance with the international treaties of Uzbekistan or on the basis of the principle of reciprocity.

62. The country provides meaningful legal assistance in a timely manner. The competent authorities use the MLA mechanisms for providing assistance in matters involving transnational elements.

63. The LEAs effectively cooperate with foreign counterparts in matters related to extradition of criminals. Besides that, there is a practice of referring criminal cases to foreign countries for criminal prosecution. The MLA mechanism is used for asset tracing, but other forms of cooperation are prioritised.

64. The Uzbek FIU regularly exchanges information with a wide range of foreign counterparts, and the nature of such information sharing is consistent with the national ML/TF risks. The DCEC has established contacts with FIUs in over 160 foreign countries through the Egmont Group's secure channel (Egmont Secure Web). The statistics on incoming and outgoing requests and spontaneous disseminations demonstrate a balanced approach used by the Uzbek authorities for requesting and obtaining information through the FIU channels.

65. Customs authorities interact with 37 countries under 137 bilateral international treaties on cooperation and mutual assistance in customs matters. International cooperation includes exchanging information, including criminal intelligence, and the organization and conduct of joint OIMs.

66. International cooperation pursued by the Uzbek supervisory authorities is limited. The financial supervisors are parties to the international agreements and members of other relevant international organizations, and there are no legislative impediments for information exchange. However, only the CB actually cooperates on AML/CFT issues with its foreign counterparts.

67. All competent authorities are able to obtain and provide information on BOs through MLA channels, but there is no common understanding of the sequence of actions that should to be taken in such cases.

Priority Actions

The following is recommended to the Republic of Uzbekistan:

1. Ensure that NRA is kept up to date, and during the next update to conduct a detailed, comprehensive analysis of the shadow economy, which is a significant country factor for ML, and its impact on ML/TF risks, as well as to pay attention to identifying threats and instances of TF within the country.
2. Make greater use of FIU resources in conducting parallel financial investigations, identifying ML and tracing the proceeds of crime for further confiscation.
3. Take further measures to enhance the effectiveness of the LEAs in detecting, disrupting and prosecuting ML, increasing efforts to identify complex ML schemes and ML by third parties (including professional laundering). Review practices (with appropriate legislative provisions where necessary) to ensure that ML can be prosecuted independently from the prosecution of the predicate offence.
4. To ensure the effectiveness and proportionality of sanctions, ensure that the range of sanctions applicable to individuals for ML is proportionate and expanded. Establish a mechanism to effectively apply proportionate and dissuasive sanctions to legal persons in cases of ML/TF schemes involvement.
5. Legislate confiscation as a legal consequence of predicate offences and ML/TF, consider expanding the use of non-conviction based confiscation.
6. Continued efforts are needed to counter TF, including identifying domestic sources of funding and conducting careful parallel financial investigations, especially where there are no apparent signs of self-financing.
7. Improve the referral of proposals to include individuals to the relevant UN sanctions lists.
8. Ensure regular updating SRA of NPO, use all possible sources to identify NPOs at risk of TF, consider developing additional specific targeted measures for vulnerable NPOs.
9. Continue work with FIs and DNFBPs to understand ML/TF risks and strengthen information exchange with the DNFBP sectors. Conduct a risk assessment of independent legal practitioners (not lawyers) and accounting service providers to determine whether they should be included in the AML/CFT/CPF system.
10. Extend the AML/CFT legal requirements to the activities of mobile network operators, transferring money, and central depository, stock exchange, and commodity exchanges.
11. To raise the level of understanding of the ML/TF vulnerabilities of legal persons among supervisors who are less aware of it, and to ensure an appropriate level of understanding among their supervised entities. To continue similar work among FIs and DNFBPs on a regular basis.
12. To study the market of professional service providers (accountants, lawyers), to assess vulnerabilities of their possible misuse. To strengthen control so that all DNFBPs, especially those who do not understand how to identify BO (except for notaries, lawyers and auditors), get this understanding and are able to do so. To amend the legislation to allow the PSA to sanction applicants for providing inaccurate information in the registration, and, if possible, make these sanctions stricter.
13. Increase the use of MLA and other forms of cooperation to trace, seize and confiscate the proceeds of ML/TF.
14. Ensure quality collection of the comprehensive and up-to-date AML/CFT statistics.

Effectiveness and Technical Compliance Ratings

Effectiveness Ratings

IO.1 Assessing risks and applying a risk-based approach	IO.2 International cooperation	IO.3 Supervision	IO.4 Preventive measures	IO.5 Legal persons and arrangements	IO.6 Financial intelligence
Substantial	**Substantial**	**Moderate**	**Moderate**	**Moderate**	**Substantial**

IO.7 ML investigation and prosecution	IO.8 Confiscation	IO.9 TF investigation and prosecution	IO.10 TF preventive measures and financial sanctions	IO.11 PF financial sanctions
Moderate	**Moderate**	**Substantial**	**Substantial**	**Substantial**

Technical Compliance Ratings

National AML/CFT policies and coordination

R.1	R.2
LC	**C**

Money laundering and confiscation

R.3	R.4
LC	**LC**

Terrorist financing and financing of proliferation

R.5	R.6	R.7	R.8
LC	**PC**	**PC**	**PC**

Preventive measures

R.9	R.10	R.11	R.12	R.13	R.14
LC	**LC**	**LC**	**PC**	**LC**	**LC**
R.15	**R.16**	**R.17**	**R.18**	**R.19**	**R.20**
LC	**LC**	**LC**	**PC**	**LC**	**C**
R.21	**R.22**	**R.23**			
LC	**PC**	**LC**			

Transparency and beneficial ownership of legal persons and arrangements

R.24	R.25
LC	PC

Powers and responsibilities of competent authorities and other institutional measures

R.26	R.27	R.28	R.29	R.30	R.31
PC	LC	LC	C	C	C
R.32	**R.33**	**R.34**	**R.35**		
C	LC	LC	PC		

International cooperation

R.36	R.37	R.38	R.39	R.40
LC	C	LC	C	LC

MUTUAL EVALUATION REPORT

Preface

68. This Report summarizes the AML/CFT/CPF measures in place in the Republic of Uzbekistan as of the date of the on-site visit. It analyzes the level of compliance with FATF 40 Recommendations and the level of effectiveness of the AML/CFT system of the Republic of Uzbekistan and recommends how the system could be strengthened.

69. This evaluation was based on the 2012 FATF Recommendations and was prepared using the 2013 Methodology. The evaluation was based on information provided by the Republic of Uzbekistan in response to the technical compliance questionnaire, and information obtained by the evaluation team during its on-site visit to the country from June 14, 2021, to July 2, 2021.

70. The evaluation was conducted under the second round of the EAG mutual evaluations by the assessment team composed of:

- Mrs Anna Iglikova (Republic of Belarus);
- Mrs Anzhelika Khadanovich (Republic of Belarus);
- Mr Yerkegali Yedenbayev (Republic of Kazakhstan);
- Mr Alexey Fomichev (Russian Federation);
- Mr Fedor Ivanov (Russian Federation);
- Mr Behrus Izatulloev (Republic of Tajikistan);
- Mr Nikita Bobryshev (EAG Secretariat, till October 1, 2021)
- Mr Dzmitry Varabyou (EAG Secretariat);
- Mrs Nazerke Zhampeiis (EAG Secretariat, from October 1, 2021).
- Mr Mikhail Kolinchenko (EAG Secretariat);
- Mr Mirzosharif Sharipov (EAG Secretariat).

71. The representatives of the EAG observers: the Republic of Armenia, the Eurasian Economic Commission and the FATF Secretariat acted as reviewers of the report.

72. The previous mutual evaluation of the Republic of Uzbekistan was conducted in 2009 using the 2004 FATF Methodology. The mutual evaluation report (MER) was adopted by the 12th EAG Plenary meeting in June 2010. The report is a public document accessible on the EAG website[2].

73. Based on the results of the first mutual evaluation, the Republic of Uzbekistan was placed in the EAG regular follow-up process. In June 2016, Uzbekistan presented the 5th detailed follow-up report at the 24th EAG Plenary Meeting for exiting the EAG follow-up process. Following the discussion, the Plenary concluded that Uzbekistan addressed the deficiencies in the implementation of the Core and Key Recommendations, and the level of technical compliance of these recommendations was assessed as corresponding to “largely compliant" (LC). The 5th follow-up report is available on the EAG website[3].

[2] https://bit.ly/3aZ8baA
[3] https://eurasiangroup.org/files/Mutual%20Evaluation/FR_2016_1_rev_1_eng.pdf

CHAPTER 1. ML/TF RISKS AND CONTEXT

General Information

74. The Republic of Uzbekistan is located in Central Asia between Amu-Darya and Syr-Darya rivers and has an area of 448,900 square kilometrers.[4] Uzbekistan stretches 930 kilometrers from north to south and 1,425 kilometrers from west to east. With a 6,221km long national border, Uzbekistan shares a 2,203km border with Kazakhstan to the north and northwest; a 1,099km border with Kyrgyzstan to the east; a 1,161km border with Tajikistan to the southeast; a 1,621km border with Turkmenistan to the west; and a 135km border with Afghanistan to the south. Most of the country's territory features deserts, steppes and mountains. Uzbekistan is a landlocked country.

75. As of January 1, 2021, the population of Uzbekistan stood at 34,560,000 people, with 17,510,000 people residing in urban areas and 17,048,000 people living in rural areas.[5]

76. Uzbekistan is a sovereign democratic republic with a presidential form of government. The Republic of Uzbekistan is a secular unitary state with some features of the federal system, as it includes the Republic of Qoralqalpogiston. Uzbekistan declared itself an independent state in August 1991.

77. In terms of the administrative division, Uzbekistan is composed of regions, districts, cities, towns, villages, and includes the Republic of Qoralqalpogiston.[6] The laws of the Republic of Uzbekistan are binding in the territory of the Republic of Qoralqalpogiston.

78. The Republic of Uzbekistan is not part of any supra-national jurisdiction and has no territories or regions with different AML/CFT regimes in place or any territorial issues that could affect the mutual evaluation.

79. The country's supreme law is the Constitution of the Republic of Uzbekistan whiich was adopted on October 8, 1992 with subsequent amendments.

80. The President of the Republic of Uzbekistan is the head of the state. Oliy Majilis (the Parliament) is the supreme public representative body exercising legislative power. Oliy Majilis is composed of two chambers – the Legislative Chamber (lower chamber) and the Senate (upper chamber). The presidential and parliamentary elections are held once in five years. There are seven political parties in Uzbekistan, five of which are represented in the parliament.

81. The executive power is exercised by the Cabinet of Ministers of the Republic of Uzbekistan (CM), which is composed of the Prime Minister, Deputy Prime Ministers, Ministers and Heads of the State Committees and also the Head of the Government of the Republic of Qoralqalpogiston.

82. The Republic of Uzbekistan is a fully-fledged international actor and subject of international law. Its foreign policy is based on the national Constitution and the principles of sovereign equality of the states, non-use of force or threat of force, territorial integrity and inviolability of existing borders, non-interference in domestic affairs of other states and other universally recognized principles and rules of international law.

83. Uzbekistan has hadfull membership in the UN since March 2, 1992. It is one of the founders of the Central Asian Regional Information and Coordination Center for Combating Illicit Trafficking of Narcotic Drugs, Psychotropic Substances and their Precursors (CARICC). Besides that, Uzbekistan is a member of the Commonwealth of Independent States (CIS), the Shanghai Cooperation Organization (SCO) and the Council of Heads of Financial Intelligence Units of CIS Member Countries (CHFIU). The Republic of Uzbekistan has observer status in the Eurasian Economic Union (EAEU).

84. The Republic of Uzbekistan is a member of the Eurasian Group on combating money laundering and financing of terrorism (EAG) since 2005.

---

[4] https://constitution.uz/ru/pages/aboutuzbekistan

[5] https://api.stat.uz/api/v1.0/data/hududlar-boyicha-shahar-va-qishloq-aholisi-soni?lang=ru&format=pdf

[6] http://web.stat.uz/open_data/ru/13.1%20Administrative-territorial%20division%20of%20the%20Republic%20of%20Uzbekistan_rus.pdf

ML/TF Risks and Scoping of Higher Risk Issues

Overview of ML/TF Risks

85. According to the State Statistics Committee of the Republic of Uzbekistan, the number of all recorded crimes has been decreasing in recent years, except for 2020.[7] In particular, 73,692 criminal offences were recorded in 2017; 49,011 criminal offences were reported in 2018; and 46,089 criminal offences were registered in 2019. Only in 2020, the number of recorded criminal offences grew (62,081 offences were detected), which could partly be caused by the negative impact of the COVID-19 pandemic - in particular, the number of fraud-related offences increased by 65.6% compared to the previous year (10,496 in 2020 versus 6,321 in 2019).

Table A. Quantity of identified ML/TF and predicate offences

	2016	2017	2018	2019	2020
ML	90	88	73	39	48
TF	7	14	9	11	4
Predicate offences	32467	29263	17868	17543	
Approximate total damage from the predicate offences (billion soums/≈million USD)	2176,6 675,5	1713,7 210,1	847,5 101,3	1681,8 176,3	

86. The offences against property (theft, mugging, robbery and fraud) accounted for 1/3 of the total number of commited criminal offences. The number of drug-related offences is also significant (18042 for the period from 2016 to 2020).

87. In the NRA, illicit drug trafficking, violation of the trade and service provision regulations, corruption (i.e. bribery), tax and customs crimes, unlicensed business activities and organized crime are assessed as posing a high and very high threat.

88. The geographic vulnerabilities of Uzbekistan are assessed as high in view of the illicit drug trafficking flows, operation of illegal armed groups, extremist and terrorist activities in some neighbouring countries and the large number of initiated criminal proceedings related to cross-border smuggling of narcotic drugs.

89. Such factors as a huge volume of cash payments, the large size of the shadow economy and large-scale cross-border importation and exportation of cash are also considered as vulnerabilities. A lot of the Uzbek nationals work abroad and are exposed to the risk of involvement in illegal activities that also contribute to the emergence of risks (remittances, cash couriers etc.).

90. The ML risks associated with corruption and bribery, tax and customs offences, illicit drug trafficking, organized crime and fraud are assessed as very high, while the ML risks related to violation of the trade and service provision regulations are rated as high. The banking sector, NBCI and DPMS sectors are classified as highly vulnerable to ML, while lawyers, notaries, and real estate agents are classified as medium vulnerable. Other sectors have a low degree of vulnerability.

91. Since the start of the armed conflicts in Syria and Iraq, more than 2,000 Uzbek nationals have travelled to these territories to fight on the side of terrorists. The high TF risk factors include labour migration, high level of TF activities in neighbouring countries, the establishment of terrorist organizations, etc. The overall level of TF threat is assessed as high.

92. No instances of misuse of NPOs for TF purposes have been recorded. The risk mitigation factors in the NPO sector include the statutory monitoring of receipt and targeted use of gratuitous aid (funds and assets) provided both domestically and from abroad.

93. The NRA lacks the assessment of the virtual asset sector, although the operation of cryptocurrency exchanges is permitted in the territory of Uzbekistan since the end of 2018. This shortcoming was eliminated in 2021, when the Interagency Commission (IAC) on April 12, 2021, adopted the

[7] https://api.stat.uz/api/v1.0/data/royxatga-olingan-jinoyatlar-soni?lang=ru&format=pdf

cryptoasset sector risk assessment report with a detailed description of threats and vulnerabilities existing in this sector and assessments of the associated risks. Based on the SRA analysis, ML risks involving the use of VA are at a low level. Such factors as the difficulties of identifying ML perpetrators using VA, the possibility of decentralised VA turnover and anonymous transactions which cannot be traced, have a sustainable influence on the risk level. At the same time, there are high risks of using VA in predicate offences, particularly TF, illegal exchange of VA, "shadow economy", and Ponzi schemes.

National Risk Assessment

94. The national money laundering and terrorist financing risk assessment (NRA) was conducted pursuant to the IAC resolution dated July 11, 2019. The NRA report was adopted by the IAC decision dated December 30, 2019.
95. It should be noted that the work aimed at the assessment of ML/TF risks in certain sectors has been already launched prior to the preparation for the NRA. In particular, the ML/TF risk assessments were conducted in some of the FI sectors (banking sector, non-bank credit institutions (NBCI) sector, insurance sector, securities sector, postal remittance sector) as well as in certain DNFBP sectors (auditors, notaries and lawyers) in 2018-2019. This work also continued after the adoption of the NRA report: the DPMS sectoral risk assessment (SRA) report was drafted in 2020, the VAs sectoral risk assessment report was adopted in 2021, and the sectoral risk assessment in the real estate agents sector is currently underway.
96. Representatives of the private sector of Uzbekistan were actively engaged in the NRA exercise. All supervisors disseminated the relevant questionnaires to their respective supervised entities, and the received responses were analyzed and provided to the FIU. The final NRA report reflects the concerted position of all competent ministries and government agencies of the Republic of Uzbekistan.
97. The last section of the NRA contains the exhaustive list of measures aimed at mitigating the identified risks. The set-out measures are ranked in order of priority of their implementation depending on the level of the relevant risks.
98. The unclassified NRA findings were published for the general public on the websites of the FIU and the supervisory authorities and communicated to financial institutions and DNFBPs. The full version of the NRA report was disseminated to the ministries, government agencies and all supervisory authorities.
99. The assessment team agrees with the NRA findings related to ML risks and considers them well-substantiated. However, it was concluded during the on-site visit that the level of threats posed by such categories of predicate offences as fraud and robbery/theft was underestimated. Besides that, the NRA lacks the assessment of extent and frequency of use of certain typologies (schemes) for laundering proceeds of particular categories of predicate offences.
100. The assessment of the NPO sector in the NRA was insufficiently detailed despite the importance and vulnerability of this sector, but Uzbekistan addressed these shortcomings by conducting the SRA of the NPO sector in 2020.

Scoping of Higher Risk Issues

101. In the process of mutual evaluation, the assessors focused on how the FIU conducts operational and strategic analysis, and on how the analysis findings are disseminated to and used by the competent authorities and the private sector entities.
102. According to the NRA, the level of ML threats posed by corruption and bribery offences is very high. In this context, the assessors paid increased attention to understanding by the private sector of ML/TF risks associated with the provision of services to PEPs, and to the effectiveness of measures applied by the private sector entities for mitigating these risks.

103. The Uzbek authorities have acknowledged the need for implementing and developing the VAs-related services and activities, including mining. The country takes measures for the development of this sector (one license was issued to the VAs exchange). The assessors paid enhanced attention to the assessment of this sector.

104. The analysis of the presented statistics on the number of identified ML offences broken down by the types of associated predicate offences (ML threats) and comparison of these data with the threat levels assigned in the NRA report shows that some types of threats may be underestimated. Therefore, the assessors paid increased attention to measures taken by the LEAs for identifying instances of legalization of proceeds of predicate offences posing high and very high levels of threat.

105. The statistics on the identified ML offences demonstrate that, in most cases, these offences are detected by the DCEC (FIU). However, all LEAs involved in AML/CFT should be obliged to identify ML offences depending on their jurisdiction over the associated predicate offences. In this context, the assessors examined and assessed how effectively the LEAs, apart from the FIU, are involved in the identification and disruption of ML offences and in conducting parallel financial investigations, including the MIA which is legally responsible for conducting preliminary criminal investigations into ML cases.

106. The assessors focused on how parallel financial investigations are conducted and how complex ML schemes are identified and investigated in practice since the initial information provided by the country indicated limited powers and capabilities of the LEAs to thoroughly examine financial elements of criminal offences.

107. In view of a significant number of ML convictions where courts imposed more lenient sentences below those provided for in the CC, the assessors thoroughly analyzed to what extent the punishments imposed by courts reflect the level of public danger of certain types of ML offences, including those associated with high-risk predicate offences.

108. In Uzbekistan, confiscation of property is not part of the substantive law and is not provided for in the criminal legislation as a legal punishment tool. In this context, the assessors paid increased attention to the application of property confiscation mechanisms at all stages of this process, starting from the application of provisional measures at the pre-trial stage and management of confiscated property through monitoring of the use of confiscated assets appropriated to the state budget.

109. Since the bulk of STRs are filed by banks, the assessors focused on understanding by non-banking credit institutions (NBCIs) and DNFBPs of ML/TF risks, arrangement of risk-based supervision and compliance with the STR reporting and record keeping requirements.

110. The assessors also paid increased attention to measures taken for enhancing the transparency of beneficial ownership and ensuring prompt access of the LEAs to the BOs information.

Materiality

111. Uzbekistan is a major economy in Central Asia, with substantial reserves of natural resources and the potential to increase their production. In 2018-2019, Uzbekistan produced about 100 tons of gold annually. The country ranks 11th in the world among gold producing countries (World Gold Council, 2020[8]). Uzbekistan has significant reserves of silver, copper, uranium, tungsten, coal, and natural gas.

112. The gross domestic product of the Republic of Uzbekistan in 2020 was UZS 602,551.4 billion (about USD 56.286 billion).[9]

Table B. Gross domestic product of Uzbekistan.

Gross domestic product of the Republic of Uzbekistan (in current prices, billion soums)				
2017	2018	2019	2020	2021

[8] https://www.gold.org/goldhub/data/historical-mine-production
[9] https://api.stat.uz/api/v1.0/data/iqtisodiy-faoliyat-turlari-kesimida-yaim-hajmi-if?lang=ru&format=pdf

				(January-June)
317,476.4	424,728.7	529,391.4	602,551.4	318,472.0

113. Uzbekistan's economy grew at an average of 6.6% over 2011-2019. Uzbekistan's largest trading partners are China, Russia, Turkey and Kazakhstan.

114. The structural transformation and economic reforms initiated in 2017 by Uzbekistan's leadership have markedly transformed the country's economy: it has opened up (integration into the system of global economic relations, improvement of the investment climate, etc), the business environment, prices, trade and foreign exchange markets have been liberalized, investment in fixed capital has increased, and the country is committed to increasing the production of high value-added goods and export diversification.

115. Among the industries, the leader is metallurgy, including ore mining and metal production (21.6%). Agriculture is also of key importance to Uzbekistan's economy (26.1%). Arable land designated for agricultural use accounts for about 10% of the country's territory. The main share of agricultural crops is the production of cotton, fruits and vegetables, and cereals (wheat, rice, corn).

116. Other industries of importance include the food industry (11.5%), automotive (9.2%), light industry (11.8%), and mining (9%).[10]

117. Uzbekistan is not a regional or international financial center.

118. There are 22 free economic zones (more than 10 industrial and agricultural, 7 pharmaceutical, as well as free economic zones in the sphere of tourism, transport logistics and sports equipment production). Their activities are based on the Laws "On Free Economic Zones" of 1996 and "On Special Economic Zones" of 2020. The first free economic zone was established in 2008, and the last one – in September 2019.

119. With the adoption of Presidential Decree No. UP-5177 of September 2, 2017 "On Priority Measures to Liberalize the Foreign Exchange Policy", an active phase of radical reform of the foreign exchange regulation system began. It should be noted that before the adoption of measures aimed at liberalizing exchange rates, the situation in the foreign exchange market of Uzbekistan was characterized by the existence of a "black" foreign exchange market, an unofficial exchange rate, which differed from the official one up to two times, limited access of entrepreneurs to the official mechanisms of foreign exchange and repatriation of profits of foreign investors.

120. Uzbekistan has established an effective mechanism for monitoring foreign trade transactions that minimises capital outflow and ML risks using import contracts. This monitoring is carried out through the Unified Electronic Information System for Foreign Trade Operations (UEISFTO) to which the State Customs Service, State Tax Service, Central Bank and banks have access (Decree of the SCS, STS, Central Bank of 12.06.2013 No. 2467 and Decree of the Cabinet of Ministers of 14.05.2020 No. 283). In particular, business entities enter information on foreign trade contracts and invoices into the UEISFTO; banks compare the information in the UEISFTO with the contract and, if there are no discrepancies, make payments and enter information on payments into the UEISFTO; customs authorities compare information from the UEISFTO with information from the customs cargo declaration and enter information on the receipt of goods into the UEISFTO. The state tax authorities monitor information received from banks and state customs authorities based on information available in electronic information bases, as well as other information available to the tax authorities. If the monitoring reveals dubious transactions involving the unjustified transfer of funds abroad or the overstatement (understatement) of the value of goods during customs clearance or other offences, materials are sent to law enforcement agencies and appropriate measures are taken.

121. In addition to effective control of non-cash movements abroad, the Currency Regulation Act prohibits the export of cash currency from the country by legal entities with the exception of banks.

[10] https://eabr.org/upload/EDB_2021_Report_Uzbekistan_and_the_EAEU_rus.pdf

122. The key role in the financial sector of the economy of Uzbekistan is played by banks with state participation (their share in the assets of the banking system is 85%). At the beginning of 2021, there were 32 banks in the country.[11]

123. In 2020, the volume of banking cash turnover was UZS 360.1 trillion, having increased by 25.4% compared to 2019. Receipts from the sale of goods and paid services accounted for about 48%, which indicates a wide circulation of cash in the country.[12] As of January 1, 2021, the total volume of cash in circulation amounted to UZS 24.9 trillion (23.2% of total money supply and 4% of GDP), having increased by UZS 674 billion compared to the same period in 2020.

124. As of January 1, 2021, over 25.776 million bank payment cards (BPC) were in circulation in Uzbekistan (01.01.2020 – 20.547 million, 01.01.2019 – 17.686 million)[13].

125. In 2019, at the initiative of the UNDP (United Nations Development Program), a study was conducted in Uzbekistan to estimate the size of the shadow economy using direct and indirect methods. It concluded that the size of Uzbekistan's shadow economy could range between 40% and 50% in relation to GDP.[14] The estimates of the state authorities are similar (UZS 245 trillion or 48% of GDP).[15] To combat this phenomenon, a number of measures have been developed and approved by Presidential Decree No. UP-6098 of October 30, 2020 "On Organizational Measures to Reduce the Shadow Economy and Increase the Efficiency of Tax Authorities".[16]

126. An urgent problem for Uzbekistan is the lack of jobs. The unemployment rate in the country increased to 10.5% in 2020 from 9% in 2019. The lack of jobs inside the country forces Uzbek citizens to work abroad. In 2020, about 1.9 million people, 14.5% of those employed in the economy, left the country[17].

127. The Agency for External Labor Migration of Uzbekistan estimated the number of migrant workers at 2.6 to 3 million in 2019 (Review.uz, 2019[18]). Up to 80% of them work in the Russian Federation and about 15% in Kazakhstan. The rest are in Korea, Turkey and other countries. In general, this is reflected in the statistics of remittances from these countries to Uzbekistan, often to support families members left behind in Uzbekistan. Total remittances to the country amounted to about 10% of the country's GDP in 2018. At the same time, there is a continuing upward trend in both the number of remittances and their volume.

128. The World Bank estimates the income of the population as "below average". At the same time, it is noted that remittances from labour migrants who have left to work in other countries contribute significantly to the increase in the level of income.

Structural Elements

129. Despite the country's ongoing structural and economic reforms since 2017, the key structural elements for an effective AML/CFT regime are already in place in Uzbekistan. The ongoing changes are more focused on improving the efficiency of the system and the coordination of its participants. The political system and institutional environment are stable. There is a high-level commitment to AML/CFT activity. Significant efforts are being made to ensure government accountability, enforce the rule of law and strengthen the independence of the judiciary[19].

[11] https://cbu.uz/ru/statistics/bankstats/452085/
[12] https://cbu.uz/ru/press_center/reviews/430110/
[13] https://cbu.uz/ru/payment-systems/interbank-calculations/
[14] https://review.uz/post/vzov-tenevoy-ekonomiki
[15] https://t.me/soliqnews/4666
[16] https://lex.uz/ru/docs/5073461
[17] https://mehnat.uz/ru/news/uroven-bezraboticy-v-uzbekistane-s-132-procenta-snizilsya-do-111-procenta
[18] https://review.uz/post/chislo-trudoviyx-migrantov-iz-uzbekistana-sostavlyaet-26-millionov-chelovek
[19] https://lex.uz/docs/3050494

Background and Other Contextual Factors

130. Uzbekistan established its AML/CFT regime in 2004 when Law No. 660-II of 26.08.2004 was adopted, defining measures to combat ML/TF and regulate the existence of a specially authorised body (FIU) in the field of AML/CFT. Since that time, the existing AML/CFT regime has been significantly developed, and the powers of the FIU have been expanded considerably.

131. In recent years, Uzbekistan has been undergoing major reforms and changes to improve its financial attractiveness on the global stage, liberalise business, and involve society in socio-political events and processes. These changes began after the change of political leadership in the country and continue to the present day.

132. Corruption remains a significant problem for Uzbekistan. The degree of threat of ML from corruption crimes in the NRA is assessed as very high. But it should be noted that the ongoing reforms have a certain positive effect, which is confirmed by the trend of improving the country's rating in the Corruption Perception Index of Transparency International (2018 - 158th place, 2020 - 146th place).[20]

AML/CFT Strategy

133. General objectives of the government and state bodies are defined in the Strategy of actions in five priority areas of development of the Republic of Uzbekistan in 2017-2021 approved by Presidential Decree No. UP-4947 of 07.02.2017. As such, the priority areas are defined as: (i) improving the system of state and social development; (ii) ensuring the rule of law and further reforming of the judicial and legal system; (iii) development and liberalization of the economy; (iv) measures aimed at ensuring security, interethnic harmony and religious tolerance, as well as at implementing a balanced, mutually beneficial and constructive foreign policy.

134. As part of ensuring the rule of law, it is envisaged to strengthen organizational and practical measures for combating religious extremism, terrorism and other forms of organized crime, improving organizational and legal mechanisms for countering corruption and increasing the effectiveness of anti-corruption measures;

135. As a follow-up to the abovementioned strategy, the Strategy of Development of the National AML/CFT/CPF System of the Republic of Uzbekistan, the Action Plan for the implementation of its objectives, as well as the list of ministries and agencies involved in AML/CFT/CPF (Presidential Decree No. UP-6252 of June 28, 2021), were prepared and approved based on the NRA outcomes[21].

136. The main areas of implementation of the Strategy for the development of the national AML/CFT/CPF system of the Republic of Uzbekistan are as follows:

- mitigation of risks identified at the national level and further strengthening of state policy in the field of combating legalization of criminal proceeds, terrorist financing and the financing of proliferation of weapons of mass destruction;
- ensuring compliance of the national system in this area with international documents, as well as implementation of the FATF standards and international legal acts into the legislation of the Republic of Uzbekistan;
- further improvement of the effectiveness of state bodies in the early prevention of crimes in this area, increasing the responsibility of organizations involved in transactions in monetary funds or other assets;
- further development of cooperation and establishing a systematic dialogue with international organizations and foreign countries;

[20] https://anticorruption.uz/ru/category/international-corruption-ratings; https://www.transparency.org/en/cpi/2020/index/nzl

[21] https://lex.uz/ru/docs/5482739

- widespread introduction of modern information technologies in the formation of an integral system of all statistical data, collection, processing, analysis and their use, as well as increasing the efficiency of information exchange in this area;
- increasing professionalism of employees of state bodies involved in this sphere, as well as training and retraining of employees of organizations involved in transactions in monetary funds or other assets.

137. The Interdepartmental AML/CFT/CPF Commission (IAC) established by Presidential Decree No. PP-3947 of September 20, 2018[22], is charged with:

- continuous monitoring of the execution of certain tasks and organization of the full implementation of activities;
- involvement of leading foreign experts and specialists in the development of draft regulations;
- monthly hearing of reports on the work done and results achieved.

138. Under the auspices of the DCEC, a Risk Assessment Center (hereinafter – the Center) was established. The tasks of the Center include:

- timely detection of the facts of legalization of criminal proceeds, terrorist financing and the financing of proliferation of weapons of mass destruction through the analysis of suspicious transactions in monetary funds or other assets;
- identification of various schemes and channels of the "shadow economy" formation, including the commission of economic crimes in the fuel and energy complex, social, banking and financial, tax, transport and construction spheres;
- study of specific schemes of money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;
- mapping of high-risk areas on the basis of continuous national risk studies, as well as the development of proposals for the prevention of causes contributing to their emergence;
- ensuring rapid exchange of information between government agencies and organizations conducting transactions in monetary funds or other assets.

139. Besides that, the National Security Strategy (a classified document) and the National Strategy of the Republic of Uzbekistan for Countering Extremism and Terrorism for 2021-2026 [23] are currently in effect, and amendments to other legislative acts are being introduced.

Legal & Institutional Framework

140. The legal system of Uzbekistan belongs to the so-called family of Romano-Germanic law. The main source of law is normative legal acts (NLAs), such as:

- Constitution;
- laws;
- resolutions of chambers of the Oliy Majlis;
- Presidential decrees and resolutions;
- resolutions of the CM;
- orders and resolutions of ministries, state committees and departments;
- decisions of local state authorities.

141. The Constitution has the highest legal force among legislative acts. Laws of the Republic of Uzbekistan and other NLAs shall be adopted on the basis of and in implementation of the Constitution and may not contradict its norms and principles.

[22] https://lex.uz/ru/docs/3912611
[23] https://lex.uz/ru/docs/5491628

142. Decrees and resolutions of the President of the Republic of Uzbekistan, resolutions of the CM, orders and resolutions of ministries, state committees and departments, and decisions of local state authorities are by-laws.

143. In case of discrepancies between NLAs, the NLA of higher legal force shall apply. In case of discrepancies between NLAs of equal legal force, as a general rule, the provisions of the normative legal act adopted later shall apply.

144. Control over the constitutionality of NLAs is exercised by the Constitutional Court.

145. The AML/CFT/PF legislation of Uzbekistan is not limited to the AML/CFT Law, which defines the main directions and measures of AML/CFT/PF and the powers of the FIU. It is a collective concept, which includes both the underlying law and other legal acts. For example, the CC contains provisions defining ML, FT and predicate offences and sets out the penalties for such crimes. The CPC includes governing asset seizure and confiscation. Numerous by-laws contain provisions governing ICR. The AML/CFT/PF legislation also includes the Strategies mentioned above and a significant number of other documents, which have been reviewed by the experts and which are referred to in the report. Thus, the AML/CFT/PF legislation of the Republic of Uzbekistan covers almost all areas of legal regulation and is comprehensive.

146. The responsibilities of the FIs and DNFBPs are set out in the AML/CFT Law and are also set out in the Presidential Decrees, CM Resolutions and ICRs, which are approved for each sector by a joint order of the supervisory body and the DCEC. The ICRs are an essential component of the AML/CFT legislation of the Republic of Uzbekistan and are mandatory for all entities in relation to which they establish obligations.

147. In the Republic of Uzbekistan, steps are constantly being taken to improve the legislation in the field of AML/CFT/CPF. The AML/CFT/CPF Law was substantially amended by Laws No. ZRU-516 of January 15, 2019 and ZRU-640 of October 5, 2020[24], as part of improving the effectiveness of the national system.

Ministries

148. Pursuant to Article 8 of the AML/CFT/CPF Law, transactions in monetary funds or other assets shall be controlled by a specially authorized body.

149. Such specially authorized state body on AML/CFT/CPF issues is the DCEC (FIU) established on the basis of Presidential Decree No. UP-5446 of 23.05.2018 by reorganizing the Department for Combating Tax and Currency Crimes and Money Laundering under the General Prosecutor's Office of the Republic of Uzbekistan.

150. The powers of the DCEC include:

- coordinating the work of organizations conducting transactions in monetary funds or other assets and bodies involved in AML/CFT/CPF;
- ensuring control over the compliance of legal entities and individuals with the requirements of the AML/CFT/CPF legislation;
- analyzing information on transactions in monetary funds or other assets in order to identify ML/TF/PF indicators;
- receiving, building and processing the database on STRs from organizations conducting transactions in monetary funds or other assets;
- making and maintaining the list of persons involved or suspected of involvement in terrorist activities or proliferation of weapons of mass destruction;
- organization of ML/TF/PF risk assessment together with involved ministries, state committees and agencies;
- suspending, for a period not exceeding thirty business days, transactions in monetary funds or other assets in order to implement AML/CFT/CPF measures;

[24] https://lex.uz/ru/docs/4163513

- analyzing and summarizing the practice of application of AML/CFT/CPF legislation;
- participation in drafting normative legal acts and international treaties of the Republic of Uzbekistan on combating the legalization of criminal proceeds, terrorist financing and the financing of proliferation of weapons of mass destruction;
- cooperation with competent bodies of foreign states, international specialized and other organizations involved in AML/CFT/CPF;
- cooperation and information sharing in accordance with international treaties of the Republic of Uzbekistan or on the basis of the principle of reciprocity with competent authorities of foreign states and international organizations involved in AML/CFT/CPF.

151. The list of ministries and agencies involved in AML/CFT/CPF is defined in the Strategy for Development of the National AML/CFT/CPF System of the Republic of Uzbekistan and includes:

- General Prosecutor's Office of the Republic of Uzbekistan (GPO) involved in supervision over the implementation of laws by the bodies involved in the fight against crime and the coordination of their law enforcement activities; maintaining the state prosecution when considering criminal cases in courts; investigation of crimes, bringing to the criminal responsibility of persons who have committed crimes.
- State Security Service of the Republic of Uzbekistan (SSS) involved in the fight against terrorism, extremism, organized crime, illegal circulation of weapons, narcotic drugs and psychotropic substances; prevention, detection and suppression of destructive activities aimed at promoting national, ethnic and religious enmity that pose a threat to state interests and security; ensuring state security in the economic and information spheres of the Republic of Uzbekistan; countering manifestations of corruption in government bodies and other organizations; conducting criminal intelligence and detective operations, pre-investigation checks and preliminary investigation.
- Ministry of Internal Affairs of the Republic of Uzbekistan (MIA) involved in criminal intelligence and detective operations, inquiry and preliminary investigation in criminal cases, including ML; combating crime and terrorism, as well as countering human trafficking; control over the circulation of industrial explosives, as well as narcotic drugs, psychotropic substances and their precursors.
- Ministry of Foreign Affairs of the Republic of Uzbekistan (MFA) that coordinates the work of ministries, departments, institutions for the development of international relations; it is involved in diplomatic and consular relations with foreign states, international, intergovernmental and regional organizations.
- Ministry of Finance of the Republic of Uzbekistan (MF) that supervises professional participants in the securities market; precious metals and stones dealers; pawnshops, points of purchase in terms of carrying out activities with precious metals and precious stones; audit organizations, auditors operating as individual entrepreneurs, providing professional services in accounting and preparation of accounting and (or) financial statements related to the performance for and (or) on behalf of the client of financial transactions; insurance organizations and insurance brokers; organizers of lotteries and electronic interactive games.
- Ministry of Justice of the Republic of Uzbekistan (MJ) that supervises notaries, organizations providing real estate services and participating in transactions related to the purchase and sale of real estate for their clients, organizations and individual entrepreneurs, lawyers and law firms providing legal services (legal assistance) related to the establishment of organizations or participation in their management, the acquisition or sale of an enterprise as a property complex, the performance of financial transactions and (or) the management of funds or other property for and (or) on behalf of the client; carries out registration and control of NPOs' activities.
- Ministry for Development of Information Technologies of the Republic of Uzbekistan (MITCD), a specially authorized, licensing and methodological body in the field of telecommunications, monitors compliance with legislation in the field of information technologies, communications and postal communication; approves, together with the DCEC, the ICRs on AML/CFT/CPF for operators and postal service providers.

- State Tax Committee of the Republic of Uzbekistan (STC) involved in suppression of sources of illegal turnover of funds, implementation, within its authority, of control over observance of legislation in conducting by legal entities and individuals of currency and export-import operations; it conducts preliminary investigations and transfer of criminal cases to LEAs according to the investigative jurisdiction.
- State Customs Committee of the Republic of Uzbekistan (SCC) that monitors compliance with customs legislation; prevents, detects and suppresses violations of customs legislation, including smuggling; participates in the system of customs and export control, one of the tasks of which is the control of dual-use items.
- State Committee on Industrial Safety of the Republic of Uzbekistan, an authorized body of state administration responsible for monitoring radiation and nuclear safety at nuclear power facilities and nuclear technologies, as well as in the field of industrial safety at hazardous production facilities; participant in the system of customs and export control, one of the tasks of which is the control of dual-use items.
- National Project Management Agency under the President of the Republic of Uzbekistan involved in licensing and supervision of persons engaged in activities in the field of circulation of virtual assets.
- Antimonopoly Committee of the Republic of Uzbekistan involved in licensing and supervision of commodity exchanges.
- Uzbekistan State Assets Management Agency (UzSAMA) that assists, including on the basis of recommendations of international financial institutions, the gradual transformation of enterprises with state participation into efficient enterprises capable of competing in domestic and foreign markets; supervises real estate organizations.
- Anti-Corruption Agency of the Republic of Uzbekistan, a specially authorized state body responsible for the formation and implementation of state policy to prevent and counter corruption, ensuring effective cooperation between state bodies and representatives of the non-governmental sector, as well as international cooperation in this area.
- Central Bank of the Republic of Uzbekistan (CB), a licensing and supervisory authority for banks, NBCIs, organizations involved in money transfers, payments and settlements (payment organizations, electronic money system operators, payment system operators).
- Bureau of Compulsory Enforcement under the General Prosecutor's Office of the Republic of Uzbekistan (BCI) that ensures unconditional enforcement of judicial acts and acts of other bodies, international cooperation in the enforcement of judicial acts and acts of other bodies.
- State Inspectorate for Control in the Sphere of Information and Telecommunications of the Republic of Uzbekistan involved in monitoring and control of the postal money transfer sector.
- State Services Agency under the Ministry of Justice of the Republic of Uzbekistan, an authorized body of state administration, carrying out activities in the sphere of providing public services to individuals and legal entities, including state registration of business entities.

Financial Sector, DNFBPs and VASPs

152. The financial sector is the most significant in the financial system of Uzbekistan in terms of assets and operations. The number of FIs tends to increase, which is linked to the ongoing reforms to open up the national economy.

Table C: Number of Financial Institutions

#	Number of Financial Institutions	2016	2017	2018	2019	2020
1	Banks	27	28	29	30	32
2	Microcredit organizations	29	30	37	56	63
3	Pawnshops	47	43	55	61	64
4	Payment service providers, e-money system operators, payment system operators	0	0	0	0	20
5	Postal communication service providers	1	1	1	1	1

6	Professional securities market participants	5	7	16	14	21
7	Insurance institutions	26	27	30	36	40
8	Commodity exchange members	1,028	1,198	1,088	1,091	1,153
9	Leasing service providers	126	126	133	137	141

Table D: Value of Transactions Carried out by Financial Institutions in 2016-2020

#	Types of FIs	2016 Transaction Value USD mln. equivalent / %		2017 Transaction Value USD mln. equivalent / %		2018 Transaction Value USD mln. equivalent / %		2019 Transaction Value USD mln. equivalent / %		2020 Transaction Value USD mln. equivalent / %	
1	Banks	277,692.0	98.6	112,823.0	97,4	102,634.0	95.9	126,377.0	96.1	200,079.2	96.47
2	Non-bank credit institutions (microcredit organizations and pawnshops)	141.7	0.1	118.2	0.1	131.8	0.1	184.	0.1	175.6	0.08
3	Payment service providers	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1,866.3	0.90
4	Postal communication service operator	84.6	0.0	56.3	0.0	40.8	0.0	47.7	0.0	46.8	0.02
5	Professional securities market participants	15.3	0.0	22.0	0.0	93.1	0.1	49.9	0.0	53.7	0.03
6	Insurers and insurance intermediaries	214.3	0.1	114.2	0.1	196.1	0.2	243.4	0.2	211.3	0.10
7	Commodity exchange members	3,363.5	1.2	2,560.3	2.2	3,647.4	3.4	4,324.0	3.3	4,791.1	2,31
8	Leasing service providers	195.2	0.1	118.6	0.1	229.4	0.2	267.1	0.2	173.8	00.8
	Total Transaction Value	281,706.6	100	115,812.6	100	106,962.4	100	131,493.2	100	207,397.9	100

153. In 2020 the total assets of banks amounted to USD 38,506.6 million (87% of FIs' assets), the volume of client operations amounted to USD 200,079.2 million (96.5% of all FIs' operations). Banks also carry out money transfers, exchange and other payments and settlements under licence, and are professional participants in the securities market and providers of leasing services. This sector is the main barrier to the entry and turnover of criminal capital in the country.

154. The exchange trading sector is represented by two commodity exchanges and their members, with annual transaction volumes increasing from USD 2,560.29 million in 2017 to USD 4,791.12 million in 2020. It is the second most important sector after banking in terms of assets (10.9%) and transactions (2.3%). The risk of trading irregularities is one of the main risks in NRA, but the exchange trading sector has built effective barriers against its realisation.

155. The payment institutions sector is ranked by assessors as the third most important sector in terms of importance and inherent ML/TF risks. The Central Bank began licensing the sector in 2020. Transaction volumes amounted to USD 1,866.3 million (0.9%) and are currently growing dynamically. Until then, the sector was unregulated, with two payment system operators, Uzcard and

Humo, and four payment organisations operating in the country. Currently, all payment organisations provide services only in the territory of the Republic of Uzbekistan. International transfers are made through banks.

156. The share of other organisations in the FI sector is insignificant and amounts from 0.02 to 0.9% by the volume of customer transactions.

157. MCOs and pawnshops are featured by a limited spectrum of provided services and a small volume of transactions carried out by them in the financial market.

158. Microcredit organizations do not process payments, maintain accounts or accept deposits, and their activities are limited solely to the provision of microfinance services to the public (in particular microcredit, microloan, microleasing), and the share of their assets does not exceed 1% of total assets held by credit institutions. It is noteworthy that the percentage of cash loans (90%) issued by microcredit organizations far exceeds the share of cashless loans provided by them. MCOs also provide microleasing services.

159. According to the applicable legislation, pawnshops may provide services only to natural persons (both residents and non-residents), while MCOs may provide services to legal entities (only residents) and natural persons (both residents and non-residents).

160. The cellular communication service operator that provided domestic money transfer services to its customers is not subject to the AML/CFT requirements but takes limited control and oversight measures.

161. The postal remittance sector is represented just by one postal services operator – Uzebiston Pochtacy (the Uzbek Post). In practice, the postal remittance providers do not carry out money transfers for customers, although internal control rules have been developed for them.

162. In Uzbekistan, the securities sector has a non-significant level. The Central Depository is not the AML/CFT obliged entity. However, since it provides services to government-owned companies and, therefore, understands the existing risks, the Central Depository performs the AML/CFT obligations similar to those imposed on financing institutions (i.e. set out in the internal control rules). Furthermore, the Stock Exchange is also not the AML/CFT obliged entity and does not implement the AML/CFT measures, since it does not provide services directly to customers that may access the stock exchange through the investment intermediaries who are the obliged AML/CFT entities.

163. In 2020 the insurance market of Uzbekistan was served by 5 actuarial organisations, 22 assistans, loss adjusters and surveyors, 5 insurance brokers, more than 6.3 thousand employees and 8.8 thousand insurance agents. Insurance agents are not the AML/CFT obliged entities.

164. The leasing sector: in 2020, the volume of new leasing transactions amounted to UZS 1.85 trillion, and the aggregate portfolio of leasing transactions exceeded UZS 5.67 trillion. At the same time, leasing companies account for 79% of the aggregate portfolio of leasing transactions, with banks accounting for the remaining 21%.[25] All customers of leasing companies are legal entities since the provision of leasing services to natural persons is not envisaged by the legislation. Besides that, all customers of leasing companies are residents of the Republic of Uzbekistan, which is also enshrined in the law.

Table E. Number of DNFBPs

1. Real Estate entities	278
2. Audit firms	70
3. Auditors	573
4. Dealers in precious metals and precious stones: • The number of licences issued for jewellery production • Number of registered retail certificates	265 incl. legal persons - 62 680
5. Notaries (state)	5

[25] https://bit.ly/3kc18Ao

6. Notaries (private)	862
7. Lawyers' organization	2 273
8. Lawyers-entrepreneurs	4 222

165. It is impossible to compare the related volumes of DNFBPs' transactions exposed to ML/TF risks, as the transactions they carry out have a non-financial expression (transactions).

166. Given the existing ML/TF risks and threats, the sector of DPMS is the largest and most significant among the DNFBP sectors in terms of the number of entities operating in the sector and the volume of transactions carried out by them. The ML/TF NRA places the DPMS sector among the sectors posing the highest risks.

Table F. Selected DPMS sector indicators

	Volume of DPMS sector operations (in million USD) and ratio (in percentage) to total FI sector operations									
	2016		2017		2018		2019		2020	
DPMS sector	12.9	0.005%	8.4	0.007%	8.8	0.008%	14.8	0.006%	10.9	0.004%
Total volume of the FI sector	281706.6		115812.6		106962.4		131493.2		207397.9	

167. Notaries and lawyers hold second place in the DNFBP sector in terms of materiality. Notaries are obliged to notarize all real estate property transactions, while lawyers only prepare documents required for carrying out transactions that are subject to mandatory monitoring under Recommendation 22, but cannot act on behalf of their clients. . Currently, 862 private notaries and 5 state (government) notaries operate in the country. It is noteworthy that before 2019, only government notaries provided notarial services in Uzbekistan. In order to operate in Uzbekistan, lawyers must necessarily obtain membership in an official lawyers association. At present, at a total of 2,273 law firms operate in the country with 4,222 lawyers working in these firms. Both notaries and lawyers are the sectors that are mostly engaged in the AML/CFT system and demonstrate the highest level of understanding of risks and obligations among all DNFBP sectors.

168. Although notaries are mandatorily involved in the preparation of real estate transactions between individuals, the volume of such transactions is not substantial. For example, the average price of real estate objects is around USD 20,000.

Table G. Information on the average value of residential real estate sales transactions between individuals (US dollars)

2018	2019	2020	2021
15,468.2	14,312.1	13,624.4	20,966.6

169. Real estate agencies are usually not parties to real estate transactions, but rather provide professional consultancy services. As for real estate agents who are individual entrepreneurs, they are only authorised by law to provide consultancy services and cannot be parties to real estate transactions.

170. In the Republic of Uzbekistan, 278 entities provide real estate services, and the real estate agent certificates are held by 1, 849 individuals. Despite the insufficient level of oversight and supervision of this sector and a relatively low level of understanding of ML/TF risks in practice, the risk of misuse of real estate agents in ML/TF schemes is substantially mitigated since all real estate transactions between individuals shall necessarily be notarized in accordance with the applicable legislation, and also due to the fact that real estate agents are legally prohibited from being directly engaged in real estate transactions for and on behalf of their customers. Nevertheless, the real estate agents are considered the significant DNFBP sector in view of a large number of entities operating in this sector, poor oversight and supervision of the sector, and high exposure of real estate property to the risks of its misuse in money laundering and criminal proceeds investment schemes.

171. Also, as with the rest of the DNFBP sectors, the volume of services provided by realtors is not significant in the Uzbek economy (less than 0.1% of GDP) and in comparison to the FS sectors.

Table H. Real estate sector indicators

Years	Mediation of transactions with real estate and rights to real estate (amount of services mln. UZS)	on the organization of auctions for real estate objects and rights to them (amount of services mln. UZS)	on the fiduciary management of real estate assets (amount of services mln. UZS)	on information and consulting services in the real estate market (amount of services mln. UZS)	Total volume of services (amount of services mln. UZS)
2018	8,872,586.6	2,708,503.5	-	4,011,909.9	15,593,000
2019	9,834,912.9	920,749.2	3,345.0	3,810,992.9	14,570,000
2020	29,771,062.6	2,561,144.7	-	2,935,792.7	35,268,000
Total	48,478,562.1	6,190,397.4	3,345.0	10,758,695.5	65,431,000

172. The Republic of Uzbekistan, in addition to DNFBPs, has identified lottery organisations as reporting entities, but the risks of these organisations are low and the materiality of the sector is minimal. In Uzbekistan, only 2 (two) organizations run lotteries, and only one of them pays out large lottery prizes (maximum USD 300,000), which occurs very rarely. Furthermore, the prizes are paid out in cashless form, and since the lotteries are run by credit institutions, they apply their internal control rules when paying out prizes as part of their payment monitoring process, which significantly reduced the risks in this sector. This sector is not considered further in the analysis as lotteries are not DNFBPs as defined by the FATF standards.

173. Auditors are almost not engaged in transactions covered by Recommendation 22, and, in terms of materiality, do not represent the important sector for the Uzbek AML/CFT system. Audit services (audit and ancillary services) are provided exclusively to legal entities, and mutual settlements for auditing services rendered are made only in non-cash form.

174. The activities of company registration services (company formation agent) are not regulated by AML/CFT/CPF legislation. At the same time, according to the applicable legislation, trusts and other similar legal arrangements cannot be established in Uzbekistan.

175. According to the accounting legislation of Uzbekistan, only specialised organisations (auditing organisations, tax advisory organisations and other organisations whose statutes provide for the provision of accounting services) may carry out book-keeping on a contractual basis. This includes processing the accounting records, which are based on primary accounting documents and do not provide the power to manage funds or bank accounts, etc., within the context of Recommendation 22. Mutual settlements for the services provided are made only in non-cash form. Individual activity of independent accountants is not permitted.

176. The activities of VASP in the Republic of Uzbekistan are not prohibited and are regulated. The UzNEX[26] is the only cryptocurrency exchange existing in Uzbekistan, but, in fact, it was not operational at the time of the on-site visit.

Preventive Measures

177. Under the AML/CFT Law, all categories of FIs and DNFBPs are subject to legal requirements and must conduct their activities in the context of preventing ML/TF violations and risks and report relevant transactions to the FIU.

[26] https://www.uznex.com/

Legal Persons and Arrangements

178. Legal persons in Uzbekistan can be created in various organizational-legal forms, the order of their creation and types (see Table I) are publicly available. The registration of legal persons is carried out by the PSC. Legal persons are subject to inclusion in the SSRBE. At a minimum, the Registry includes the TIN, data on the registering authority, date and number of registration, the name of the legal person and its type, status (active, liquidated or in the process of liquidation), the size of the authorized capital, data on the founders and their shares in the authorized capital (even if there are several founders), contacts (e-mail address, telephone number, address), information on the head (name and TIN). LLCs are the most common type of legal persons. Their number at the time of the on-site mission was more than 45% of all legal persons registered in Uzbekistan.

179. LLCs are most often used for illegal purposes, including ML, due to the simplicity of their registration; a range of activities that can be performed by LLCs; liberalization of currency policy; low requirements for the size of the authorized capital; and simplified taxation. The most typical use of LLCs for illegal purposes is cash-out. Different mechanisms can be used for this purpose. For example, transferring money from the LLC account(s) to individuals for fictitious services or by granting a financial loan in favor of a legal person or an individual. The LEAs also noted the following cases of legal persons being used for criminal purposes: a) as front companies to conceal illegal activities; b) to conceal BO through front persons; c) for tax evasion. The NRA results in terms of the above-mentioned vulnerabilities of LLCs correlate with examples of criminal cases of money laundering.

180. Trusts cannot be established in Uzbekistan. At the same time, the legislation provides for relations between foreign trusts and residents to receive income for their benefit. At the time of the on-site mission, there were relations between foreign trusts and residents.

Table I: Number of Legal Persons Registered in the Republic of Uzbekistan in 2016-2020

#	Form of Incorporation of Legal Persons	2016	2017	2018	2019	2020
1	Private companies	6,245	4,834	8,384	18,664	12,425
2	Family businesses	2,863	2,266	4,432	13,054	17,958
3	Farming enterprise	48,727	13,072	18,770	8,904	9,939
4	Dekhan farm	2,362	828	882	1,287	1,033
5	Limited liability companies	21,893	17,007	35,699	60,693	61,664
6	Supplementary liability companies	0	29	30	30	9
7	Joint stock companies	17	5	16	23	15
8	Unitary enterprises	91	250	308	281	156
9	Government-owned unitary enterprises	27	163	154	66	23
10	Production cooperatives	5	71	28	143	1110
11	General partnerships	4	2	1	3	1
12	Limited partnerships	2	0	0	1	3
13	Total	82,236	38,527	68,704	103,149	104,336
14	Companies with foreign investment	715	284	830	971	595
15	Number of legal persons excluded from the Register[27]	25,432	22,066	15,713	15,777	7,887

Supervisory arrangements

181. In accordance with the AML/CFT Law, the DCEC ensures control over the implementation by legal entities and individuals of the requirements of the legislation on combating the legalisation of proceeds of crime, TF and PF.

182. All reporting entities are supervised by legally authorized state bodies and organizations.

[27] Bankruptcy; voluntary liquidation; liquidation due to inactivity since the date of government registration; termination of activity as a result of restructuring, merger or acquisition, etc.

Table J. Supervisory bodies for FI, DNFBPs and VASPs

Types of institutions	Supervisor
1. Banks	Central Bank
2. Non-bank credit institutions (NBCI) • Microcredit organizations (MCO) • Pawnshops	
3. Institutions providing remittance, payment and settlement services: • Payment service providers and e-money system operators • Payment system operators	
• Postal communication service operators • Postal communication service providers	• Ministry of Information Technology and Communications Development of the Republic of Uzbekistan • State Inspectorate for Overseeing Information Technologies and Telecommunications – monitoring and oversight authority
4. Professional securities market participants: • Investment intermediaries (brokers and depositories) • Investment consultants/ advisors • Investment funds • Investment asset managers • OTC securities market operator	Finance Ministry - from 01.05.2021 (from 2016 until 2019 - Centre for Coordination and Development of the Securities Market under the State Committee for Competition, from 14.01.2019 until 2021 - Capital Market Development Agency)
5. Insurers and insurance intermediaries: • Insurance companies • Insurance brokers • Reinsurance brokers	Insurance Market Development Agency under the Finance Ministry
6. Commodity exchange members	• Antimonopoly Committee (supervision of the commodity exchanges) - since January 2019 (since 2016 until 2019 - State Committee for Privatisation, Demonopolisation and Development of Competition) • Commodity exchanges (supervision and monitoring of their member)
7. Leasing institutions	Finance Ministry
8. Virtual asset service providers: • Cryptocurrency exchanges	National Project Management Agency under the President of the Republic of Uzbekistan
9. Real estate agencies	State Assets Management Agency
10. Audit firms 11. Auditors	Finance Ministry
12. Dealers in precious metals and precious stones	Finance Ministry (State Assay Chamber)
13. Notaries (state) 14. Notaries (private)	Justice Ministry
15. Lawyers' organization 16. Lawyers-entrepreneurs	

International Cooperation

183. International treaties of the Republic of Uzbekistan are concluded on behalf of:

- the Republic of Uzbekistan – interstate treaties;
- the Government of the Republic of Uzbekistan – intergovernmental treaties;
- state bodies within their authority – interagency treaties.

184. State bodies, within their authority, conclude interagency treaties and agreements. In all bilateral treaties of the Republic of Uzbekistan on MLA in criminal matters and extradition, the General Prosecutor's Office is designated as the central authority. The GPO, SC, as well as MIA and SSS (not requiring a court decision or prosecutor's consent (sanction) for procedural actions) are the competent authorities for MLA on the basis of the principle of reciprocity. Of great importance in the issues of international cooperation is the FIU, whose resources are used in parallel financial investigations conducted by LEAs.

185. Uzbekistan has concluded (ratified) 5 international multilateral treaties (conventions), 6 regional multilateral treaties, and 32 bilateral treaties in combating crime and MLA, including in the AML/CFT sphere. The GPO has concluded 7 legal assistance and cooperation agreements. The main partners are the CIS Member states (Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Ukraine, Belarus, etc.) and Turkey, China, etc.

186. The DCEC has established contacts with FIUs of more than 160 foreign countries through a secure channel of Egmont Group (Egmont Secure Web). The DCEC has been a member of the Egmont Group since 2011. The DCEC has signed more than 20 Cooperation Agreements and Memorandums of Understanding under the GP with foreign competent authorities.

187. Customs authorities interact with 34 countries under international treaties and agreements on cooperation and mutual assistance in customs matters.

CHAPTER 2. NATIONAL AML/CFT POLICIES AND COORDINATION

Key Findings and Recommended Actions

Key Findings

1. The Republic of Uzbekistan is making significant efforts to identify, understand and assess its ML/TF risks and develop measures to mitigate them. An NRA was conducted in 2019, and the country is reforming its public authorities and administration, including those involved in the AML/CFT system. Measures are being taken to involve the private sector in AML/CFT activities and raise civil society awareness.
2. The conclusions of the NRA regarding ML risks are reasonable, but the threat level of such categories of predicate crimes as fraud, robbery/theft seems to be underestimated.
3. The country understands the TF risks to a large extent.
4. The NRA's assessment of the NPO sector was not sufficiently detailed, but these shortcomings have been addressed in the conduct of the SRA.
5. The country is largely responsive to the risks identified through national policy changes and coordination among competent authorities. However, some of the weaknesses identified in the ML/TF risk analysis have not been mitigated.
6. FIs and DNFBPs use the findings of the NRA to justify the need for enhanced measures where a higher risk situation, based on geographical characteristics, exists in the customer profile and to determine the risk profile of transactions conducted.
7. The aims and objectives of competent authorities are largely consistent with national ML/TF risks. Competent authorities make active use of the mechanisms available to cooperate and coordinate the implementation of AML/CFT policies.
8. The country largely ensures that the findings and conclusions of the NRA are communicated to the private sector and takes necessary steps to raise awareness among the private sector of the identified ML/TF risks and measures to mitigate them.

Recommended Actions

1. Uzbekistan should keep NRA up-to-date and consider the following as part of the next NRA update:
   - Conduct a comprehensive analysis of the shadow economy and more detailed analysis of its impact on ML/TF risk;
   - Consider potential re-rating of the level of threats emanating from fraud and theft/robbery.
2. Introduce the concept of national PEPs in national legislation and assess the ML risk of such individuals.
3. Focus on identifying TF threats and risks within the country and strengthening work with the private sector to prevent potential TF incidents.

188. The relevant Immediate Outcome considered and assessed in this Chapter is IO.1. The Recommendations relevant for the assessment of effectiveness under this section are R.1 and R.2.

Immediate Outcome 1 (Risk, Policy and Coordination)

Country's understanding of its ML/TF risks

189. The Republic of Uzbekistan has made significant efforts to identify, understand and assess its ML/TF risks and develop measures to minimise them. This work has intensified significantly recently, starting in 2017. The country has been reforming its public authorities and administration, including those involved in the AML/CFT system. Measures are being taken to involve the private sector in AML/CFT activities and raise civil society awareness.

190. As a result of the reforms, several new bodies mandated to combat AML/CFT have been formed. In contrast, some existing ones have been given relevant supervisory, coordination and other powers in this area.

191. Pursuant to Presidential Resolution No.PP-3947 dated September 20, 2018, the IAC was established in Uzbekistan. The Commission is composed of the deputy heads of 23 ministries and government agencies and is chaired by the Deputy General Prosecutor of the Republic of Uzbekistan.

192. National and sectoral ML/TF risk assessments are carried out by competent authorities to identify and assess risks.

193. In accordance with the IAC resolution of July 11, 2019, the NRA was conducted in Uzbekistan. The NRA report was adopted by the IAC on December 30, 2019.

194. The methodology used to conduct the NRA is based on the FATF Guidance on National Money Laundering and Terrorist Financing Risk Assessment (2013), taking into account the World Bank, International Monetary Fund and sectoral assessments conducted in Uzbekistan and covered the period from 2016 to 2019. Two indicators were used to assess the extent of ML threats: the number of crimes and the amount of proceeds of crime generated by predicate offences. The amount of money was not taken into account for the TF threat assessment, as small amounts of money, which may also have a legitimate origin, are sufficient for TF purposes. The analysis of LEAs was based on the TF incidents, the channels used and the capabilities underlying the TF vulnerabilities.

195. Statistical information from the analysis of sentences for predicate offences, ML and FT and other analytical and criminal intelligence information from LEAs were used as sources of information for the assessment of threats. In case of insufficient information, expert assessments were used to assess threats.

196. In addition to general structural vulnerabilities based on political, geographical, economic and demographic characteristics of the country, including information from international organisations about Uzbekistan, reports on ML/TF risk assessments at the FI and DNFBP sectors level (SRA) conducted by supervisory authorities in the country, as well as statistics and sectoral regulations were used as a basis for defining vulnerabilities. Based on the threats and vulnerabilities identified, the likelihood of each threat and vulnerability being realised was derived and the possible consequences of their realisation were formulated. The comparison of probabilities and consequences allowed the Republic of Uzbekistan to identify and assess the ML/TF risks present in the country.

197. The unclassified NRA findings were published for the general public on the website[28] of the DCEC (FIU) and were also posted on the websites of the supervisory authorities and communicated to FIs and DNFBPs via various channels. The public version of the report summarises the methodological approach to the assessment, the contextual factors, the ML/TF threats, vulnerabilities and risks identified in the assessment, and the proposed mitigating measures.

198. The full version of the report containing a detailed description of the risk assessment process, the data presented, conclusions and proposed measures were communicated to ministries and agencies, and all supervisory bodies through secure communication channels. The full version of the NRA has also been made available to the private sector by supervisors and other agencies through seminars, roundtables and other events.

199. The FIU was the focal point for the NRA, the analytical materials of the DCEC were an important source of information for the NRA. Also, qualitative and quantitative statistical information was provided by all LEAs and justice agencies: information on predicate offences was provided by the SC, MIA, SCC, GPO and SSS.

200. The following information was collected within the NRA:

- court decisions (sentences);
- questionnaires of supervisory bodies for the private sector;

[28] http://new-department.uz/ru/press/news/439/

- statistical data from law enforcement agencies (MIA, SSS, GPO, SC), statistical and other information from ministries and departments;
- data from the DCEC as a LEA (facts discovered, cases prosecuted, actions taken on economic and corruption offences and others, STRs, typologies, strategic analysis, etc.);
- statistical data of the supervisory bodies.

201. At the same time, meetings with supervisors and LEAs were held during the conducting NRA to discuss selected issues related to ML/TF risks and threats.

202. The representatives of the LEAs showed the assessors sufficient awareness of the findings of the NRA and its conclusions, indicated the main ML threats and risks. They also reported that the results of the NRA had been discussed in various operational meetings in the units and had been communicated to the staff.

203. It should be noted that the work aimed at the assessment of ML/TF risks in certain sectors has been already launched prior to the preparation for the NRA. In particular, the ML/TF risk assessments were conducted in some of the FI sectors (banking sector, non-bank credit institutions sector, insurance sector, securities sector, postal remittance sector) as well as in certain DNFBP sectors (auditors, notaries and lawyers) in 2018-2019. This work also continued after the adoption of the NRA report: the DPMS and the NPO SRA reports were drafted in 2020, the VA SRA report was adopted in 2021, and the SRA in the real estate agents sector is currently underway.

204. Supervisors and most DNFBP sectors were actively involved in identifying national risks. Only representatives of the precious metals dealers and lottery sectors found it difficult to indicate their role in preparing the NRA. All supervisors' understanding of the risks is based primarily on the NRA conducted. All supervisors are aware of the findings of the NRA and support its main conclusions.

205. Representatives of the private sector of Uzbekistan were also actively engaged in the NRA exercise. All supervisors disseminated the relevant questionnaires to their respective supervised entities, and the received responses were analyzed and provided to the FIU. The final NRA report reflects the concerted position of all competent ministries and government agencies of the Republic of Uzbekistan.

206. The NRA does not include an assessment of the VA sector, although crypto-exchanges have been allowed to operate in the Republic of Uzbekistan since the end of 2018. This shortcoming was remedied in 2021 when a decision of the IAC approved an SRA for virtual assets detailing the threats and vulnerabilities of the sector and an assessment of the relevant risks. In this context, experts greatly appreciate the efforts of competent authorities in identifying and mitigating ML/TF risks in the field of virtual assets.

207. The assessment team notes, in general, that there is a significant understanding of ML/TF risks among the competent authorities, based on the findings of the NRAs and SRAs, as well as knowledge of their methodologies.

ML risks

208. The ML risks associated with corruption and bribery, tax and customs crimes, illicit drug trafficking, organized crime and fraud are assessed as a very high degree of risk, the ML risks related to violation of the trade and service provision regulations are considered to be high, while money laundering risks associated with human trafficking, unlicensed business activities, illegal trade in medicines, smuggling, acquisitions and sale of criminal property, forgery of documents, stamps and seals, illegal production of alcohol and tobacco products and environmental crimes are rated as medium.

Table 1.1. Main ML typologies identified and their frequency

№	ML typology	Frequency of use
1.	Purchase of movable and/or immovable property with the proceeds from the commission of corruption offences, drug trafficking, fraud, etc.	Very often
2.	Cash deposit to the bank's cash desk for the formation replenishment of the legal entity's statutory	Often

	fund	
3.	Granting a financial loan in favour of another legal or natural person	Often
4.	Transferring criminal proceeds *(derived from embezzlement or tax evasion)* to a foreign legal entity under the guise of payment for imported goods or services *(whose price was artificially inflated)* followed by the acquisition of movable and/or immovable property in a foreign country	Rarely
5.	Purchase of a vehicle in the name of a legal entity and its subsequent transfer to an individual	Rarely

209. Schemes related to illegal transit (including cross-border) and cashing are relevant. Considering contextual factors specific to the Republic of Uzbekistan and legislative regulation (see R.15), the risks of involvement of VASP in ML schemes were assessed as low; however, there is a high probability of exploitation of VA to commit predicate offences.

210. During the NRA, the competent authorities identified different types of vulnerabilities (geographical, political and legal, economic, social and sectoral), indicating an in-depth approach to understanding the factors and deficiencies in the system that could be exploited for ML. These include the border with Afghanistan, visa-free regimes in border areas with other countries, deficiencies in national inter-agency cooperation, the presence of a "shadow" economy, currency instability, unemployment and labour migration, corruption and sectoral vulnerabilities identified in the FS and DNFBP sectors, among others.

211. A review of the legal entities' registration, re-registration and operating procedures identified a number of vulnerabilities caused by the insufficient focus placed on them in the AML/CFT legislation, which increases the risks of their misuse for ML or TF purposes. However, such vulnerabilities are largely offset by the requirements for legal entities to make payments and settlements through deposit (current) accounts opened with Banks, which allows for effective monitoring of their transactions.

212. In addition, one of the purposes of the assessment was to assess the ML risks associated with national PEPs (due to the absence of this concept in the regulatory system of the Republic of Uzbekistan), which were assessed as high, indicating that the competent authorities understand the need to take measures to control the income and assets of such persons to prevent the possible commission of corruption offences and the laundering of proceeds of crime.

213. It should be noted that the FIU demonstrated an entire understanding of ML risks, the LEAs and the judicial authorities (SC, MIA, SCC, GPO and SSS), and the supervisory authorities in the FI sector (CB, NAPM, MITCD). DNFBP sector supervisors have also generally shown sufficient understanding of the risks identified by NRAs; however, representatives of the Assay Chamber have a weaker understanding of ML/TF risks, focusing mainly on the risk of purchasing stolen precious metal items, which nevertheless correlates with the DPMS SRA.

214. The team of assessors, taking into account the assessment findings, shares the NRA's conclusions about ML risks and considers them valid. Still, during the assessment, the threat level of predicate offence categories such as fraud, robbery/theft appears underestimated (see IO.7). The experts also believe that the extent to which specific ML typologies (schemes) used in the money laundering of particular categories of predicate offences should have been considered in more detail during the NRA.

TF risks

215. TF threats and risks faced by Uzbekistan are high. From the beginning of armed conflicts in Syria and Iraq, over 2 000 Uzbekistan citizens moved there to participate in armed clashes on the terrorist side.

216. Most TF cases included two distinct elements:

- The funds were received from legitimate sources (personal income, donations, etc.) abroad.
- Self-financing was arranged primarily by the Uzbek nationals who stayed abroad and transferred their funds by-passing the national financial system of Uzbekistan (see Case Study 1.1).

Case Study 1.1
The FIU was requested by the LEA to conduct a background check of the suspect - individual A, who bought airline tickets for travelling from the Russian Federation to Turkey by third parties.
The FIU identified that individual A was the citizen of the Republic of Uzbekistan and left Uzbekistan for the Russian Federation in 2012. It was also established that individual A bought airline tickets using the bank card issued in his name for several Uzbek nationals who were suspected of being involved in terrorist activities.
In 2017, the criminal proceedings were initiated under Article 244-2, Part I (establishment, leadership and membership in religious extremist, separatist, fundamentalist and other banned organization) of the CC.
The criminal investigation revealed that, when staying abroad, individual A came under the influence of emissaries of the Islamic State international terrorist organization. After that, individual A recruited the Uzbek nationals (primarily young people) in the foreign country and financed their travel to Syria and Iraq for joining the international terrorist organizations and participation in the hostilities.
Individual A was prosecuted under Article 155-3, Part I of the CC (TF).

217. The main identified TF typologies (schemes) involve the movement of funds through intermediaries (cash couriers, hawala, etc.), transfer of funds through the payment systems, online transfer of funds with the use of bank cards, misuse of money remittance systems and purchase of airline tickets and other travel documents for foreign terrorist fighters (FTFs). It was also found that hawala services are used in the shadow import-export schemes, which may pose threat in terms of both ML and TF.

218. The TF risk assessment considered the specificities of operation of NPOs in Uzbekistan and preventive measures taken by the Uzbek authorities as well as the geographic and social vulnerabilities existing in the country. Besides that, such vulnerabilities of the national AML/CFT system as the widespread use of cash, the popularity of money transfer services without opening bank accounts, etc., were also taken into account.

219. The FIU and LEAs have demonstrated a profound deep understanding of TF-related risks. The most solid understanding of TF risks among the supervisory authorities has been demonstrated by the CB and the MITCD, while other supervisors are also aware of the TF risks and the underlying factors. Although the level of understanding of ML/TF risks varies among the DNFBP sector entities, generally they understand the importance of the application of risk mitigation measures and fulfilment of the statutory obligations such as screening customers against the lists of designated persons and entities and denial of services.

220. The assessment team generally agrees with the country's approach to the assessment of TF risks and is of the opinion that the information obtained in the course of the on-site visit allows for making a conclusion about substantial understanding by the country of the existing risks related to terrorism and TF. However, despite the presented NRA analysis and measures taken by Uzbekistan to prevent terrorism and religious extremism in its territory, the assessors suggest that Uzbekistan should focus on the identification of TF factors and threats inside the country and more actively engage with the private sector for preventing potential TF through the country's financial system (see IO.9).

221. The assessors noted that the assessment of the NPO sector in the NRA was insufficiently detailed despite the importance and vulnerability of this sector but Uzbekistan addressed these shortcomings by conducting the SRA of the NPO sector in 2020.

National policies to address identified ML/TF risks

222. As part of the NRA, the final part of the report proposes measures to minimise the risks identified. The set out measures are ranked in order of priority of their implementation depending on the level of the relevant risks. The highest priority is given to the adoption of the National AML/CFT/CPF Strategy as well as to combating corruption, disruption of illegal payment systems, strengthening the fight against tax and customs crimes and improving transparency of FI and DNFBP transactions and customers.

223. In June 2021, Uzbekistan adopted the National AML/CFT System Development Strategy (Presidential Decree No.UP-6252 dated 28.06.2021) that set out the detailed action roadmap, and modified the powers and organizational structure of the FIU and enhanced the mechanisms of coordination among all ministries and government agencies.

224. The National Anti-Extremism and Terrorism Strategy for 2021-2026 was adopted in Uzbekistan in 2021 (Presidential Decree No.UP-6255 dated 01.07.2021).

225. In the assessors' opinion, both strategies respond to the identified country-specific ML and TF risks and trends, summarise the measures previously taken, improve the effectiveness of the national anti-money laundering system and set a unified vector for its future development. However, it is not possible to fully assess the effectiveness of its impact at the time of the on-site mission.

226. It is noteworthy that the aforementioned strategies were adopted quite recently, but the work to mitigate the identified risks had been launched before their approval.

227. For example, to decrease ML risks from committing tax and customs crimes[29], measures have been taken in Uzbekistan to reduce the size of the shadow economy and prevent tax offences in the country. With a view to implementing these measures, Presidential Decree No.UP-6089 on Administrative Measures to Reduce Shadow Economy and Improve Effectiveness of Tax Authorities was issued on 30.10.2020, which laid the foundation for the establishment and operation of the special interagency working groups, and approved the roadmap for analyzing and curbing the shadow economy. The measures aimed at improving the national system involved revision of the supervisory approaches of the STC and intensification of efforts for identifying dubious companies, which included upgrading of the analytical software, implementation of the risk-based approach, open publication of the "grey lists' of counterparties, etc.

228. To reduce ML risks of corruption and bribery[30], Law No.ZRU-149 on Combating Corruption dated 03.01.2017 and the Action Strategy on Five Priority Development Areas in 2017-2021 (endorsed by RU Presidential Decree No.UP-4947 dated 07.02.2017) were adopted, which covers the fight against corruption and extremism and prevention of predicate offences. Decree No.UP-5729 on Measures for Further Improvement of Anti-Corruption System of Uzbekistan issued by the President of the Republic of Uzbekistan on 27.05.2019 approved the Government Program on Combating Corruption for 2019-2020. With a view to strengthening the fight against corruption, the Anti-Corruption Agency of the Republic of Uzbekistan was established pursuant to Presidential Decree No.UP-5013 on Further Measures for Improvement of Anti-Corruption System of Uzbekistan dated 29.06.2020.

229. To accomplish the objectives set out in the NRA, additional foreign exchange regulatory measures were implemented. These include imposing bans on bank cards/transactions, whereby the bank cards issued in offshore zones or in AML/CFT non-cooperative countries may be carried out only through the bank POS terminals. Besides that, the CB circulated the instruction to Banks, according to which funds held in plastic cards may be cashed out through the ATMs only in the national currency, and cash may be withdrawn by residents in the national or foreign currency and by non-residents in the national currency only through the bank POS terminals.

230. An agreement on the exchange of information on passenger customs declarations and amounts of imported foreign cash in excess of the established limits was signed between the CB and the SCC.

231. To enhance measures for the identification of BOs, the procedure was introduced, according to which BO information should be indicated in the applications for government registration of legal entities and should be recorded in the SSRBE (see IO.5 for details).

232. With the view to improving the effectiveness of parallel financial investigations, the joint directive was issued in May 2021 by the GPO, MIA and SCC that set out the procedure of examination of financial aspects of criminal activities in the course of OIA, pre-investigation checks, inquiries and preliminary (pre-trial) investigations. The AML/CFT training, including parallel financing

[29] The NRA identifies as very high ML/TF risks requiring immediate measures applying.
[30] ML risks from corruption and bribery are also identified as very high.

investigation training, has been arranged for judges in the Academy of the GPO jointly with the specialists of the relevant international organizations.

233. For the purpose of regulating cryptoasset transactions, on 20.05.2021, the GPO, the MIA, the SSS and the SCC issued the joint Resolution that approved the procedure of seizure, storage and confiscation of cryptoassets in the course of pre-investigation checks, inquiries, preliminary (pre-trial) investigations and OIA. NAPM Decree No. 3 dated 08.07.2021 and ВСУС Decree No. 16 dated 07.06.2021 approved the ICR for persons engaged in operations in the field of circulation of crypto-assets

234. Based on the NRA findings, the competent authorities amended their relevant programs and strategies aimed at mitigating the identified risks within their purview.

235. The risk mitigation programs and roadmaps have been developed in line with the NRA findings. It is not possible to assess their effectiveness at this time, as they are under implementation. Also, starting from 2018, the special roadmaps for improving the risk mitigation approaches in particular sectors (banking, NBCI, commodity exchange, postal remittance sectors) have been developed based on the findings of the SRAs conducted in certain FI and DNFBP sectors, in addition to the country-wide risk mitigation measures.

236. To promptly respond to the evolving ML/TF risks, special situation centers (that also deal with PF risks) have been established within the MIA and the SCC. The FIU, in cooperation with other government authorities, has drafted amendments and adopted a significant number of regulations that govern, *inter alia*, access of LEAs to information constituting bank secrets (Law No.ZRU-697 dated 28.06.2021), AML/CFT financial investigation procedures (classified document), etc. The GPO has aligned the international cooperation priorities with the findings of the ML/TF risk assessment. The revised Law on Combating Human Trafficking (No.ZRU-633 dated 17.08.2020) was adopted at the initiative of the MIA.

237. At the same time, the individual deficiencies identified in the ML/TF risk analysis have not been mitigated. For example, the concept of national PEPs was not defined in the current legislation. The review of the provided information does not allow for making a firm conclusion that Uzbekistan comprehensively responds to the existing ML/TF threats, but indicates that the country undertakes substantial efforts to mitigate them.

238. Given the significant work undertaken to develop measures to minimise the identified risks, and taking into account the national strategic initiatives adopted since the adoption of the NRA up to the on-site mission, the assessment team considers that the country is largely responsive to the identified risks through national policy changes and coordination of competent authorities.

Exemptions, enhanced and simplified measures

239. The NRA does not apply to justify exemptions or simplified application of measures (SDD), as no such measures and exemptions are provided for in legislation.

240. The NRA investigates in detail the different types of vulnerabilities, including geographical, economic, social and sectoral vulnerabilities. FIs and DNFBPs use the findings of the NRA to justify the need for enhanced measures when a higher risk situation, based on geographical characteristics, exists in the client profile and to determine the risk level of the operations carried out. (see also R.1, R.10 and IO.4).

241. It is worth pointing out that, following the adoption of the NRA and subsequent SRAs conducted in 2020 and 2021, the relevant modifications, including those related to the higher risk criteria, have been introduced in the ICRs of certain categories of FIs, which demonstrates that the country takes active steps to address the identified risks. For example, as a result of the NRA, the AML/CFT/CPF ICR for Banks approved by a joint resolution of the Central Bank and the FIU have been amended to include not only PEPs and their family members but also persons close to PEPs as high-risk clients. Similar amendments have been made to other ICRs. In addition, the NRA resulted in changes to the ICRs for all sectors that require a systematic review, analysis and identification of potential ML/TF

risks at least once a year, documenting the review results and taking appropriate measures to mitigate the risks identified.

Objectives and activities of competent authorities

242. The activities of the competent authorities are in line with the priorities identified in the NRA. Although the National AML/CFT System Development Strategy was adopted in June 2021, the competent authorities prepared the roadmaps based on the national ML/TF risk assessment findings to address the identified risks, and the Uzbek authorities demonstrated to the assessors the results achieved since 2020: the relevant regulations were adopted, the analytical approaches were updated, the organizational structure and logistics support of certain government agencies was changed, and interagency cooperation was enhanced.

243. Furthermore, measures are taken to mitigate high-level ML threats such as corruption, bribery, tax crimes, customs offences and fraud. These efforts are pursued under the national programs and strategies adopted prior to the NRA exercise and include the following: enhancement of transparency of legal entities, reduction of the volume of cash transactions, analysis of the shadow economy, and strengthening the border controls (see above).

244. Many LEAs have modified the structure of their divisions and optimized the staff size to streamline and focus their activities on addressing the priority issues consistent with the identified risks. The Academies of the GPO and the MIA have updated their training programs for LEAs officers to reflect the recent AML/CFT trends.

245. The SSS actively counteracts terrorist and extremist activities focusing on the prevention of these criminal offences. Based on the NRA findings, the internal interagency regulations and practices were adopted to improve the quality of TF investigations. The NPO SRA was updated in cooperation with the MJ.

246. Uzbekistan has conducted the assessment of ML/TF risks associated with VA, and intense interagency efforts are undertaken to prevent misuse of VA in ML/TF schemes and to raise awareness of FIs, DNFBPs and VASPs of the VA related risks. The NAPM has been designated as the supervisory authority for the circulation of VA. Separate FIs and DNFBPs demonstrated an understanding of the need to assess risks with the use of new products and technologies prior to their launch.

247. As the ICRs for FIs and DNFBPs in the Republic of Uzbekistan are developed by the supervisory authorities and agreed upon by the FIU, all supervisors have updated the ICRs of appropriate FIs and DNFBPs in connection with identified risks and preventive measures aimed at risks mitigation. The supervisory authorities circulated the info letters with instructions on how to address the identified risks. The guidelines and recommendations on customer identification and application of CDD measures were developed. Many training events on how to mitigate risks and address other AML/CFT issues were held. The CB and the MITCD entered into agreements with the SCC for managing the cross-border and foreign cash smuggling risks.

248. The ML/TF risk mitigation roadmaps have been implemented in certain FI and DNFBP sectors, and the policies developed and pursued by the relevant supervisory authorities are primarily focused on the mitigation of these risks.

249. To enable the automated processing of incoming STRs, the FIU has updated and improved the methodology used for analyzing and prioritizing the incoming reports depending on the identified risks. In the course of preliminary automated processing of incoming reports, they are ranked against the criteria that reflect the ML/TF risks identified in the country. Analysis of incoming STRs is also prioritized depending on the level of risks identified in the received reports.

250. In general, Uzbekistan has demonstrated that it implements significant response measures that are commensurate to the identified ML/TF risks. The LEAs, including the FIU, updated their strategic plans and initiatives to reflect the NRA findings. The FIU, the SSS and the SCC developed and adopted the classified instructions, guidelines and regulations (which were nevertheless provided to

the assessment team) related to domestic cooperation with a view to strengthening AML/CFT cooperation, intensifying the information sharing process and pursuing the coordinated efforts to identify ML/TF cases.

251. Of note is the active international cooperation pursued by the competent authorities under the international and bilateral information-sharing agreements with the members of the Egmont Group, the CIS, the CHFIU and the Shanghai Cooperation Organization. The areas of international cooperation and information sharing correlate with the identified risks (see IO.2).

252. Despite the measures taken to improve the legal and regulatory framework on confiscation, assessors consider the country's efforts to detect and suppress the transfer of funds outside Uzbekistan to be insufficient, as reflected in the NRA analysis. (see IO.8).

253. Given the above, the assessment team considers that the goals and objectives of the competent authorities are largely consistent with national ML/TF risks and notes their continuous monitoring and prompt response.

National coordination and cooperation

254. Pursuant to Executive Order No.309-F issued by the CM on May 7, 2012, the Interagency Working Commission for Studying and Implementing New FATF Recommendations (IWC) and the IWC Expert Group were established. The IWC acted as the interagency AML/CFT coordination body, one of the objectives of which was to arrange for the ML/TF NRA exercise. The Expert Group identified the main risks, which were considered at the meetings of both the Expert Group and IWC. Besides that, the IWC adopted the annual working plans that included, *inter alia*, implementation of risk mitigation measures, improvement of the existing AML/CFT system and development of methodological guidelines by the ministries and government agencies.

255. In 2018, the IWC was abolished and replaced by the IAC. The IAC is the key body responsible for arranging AML/CFT/CPF cooperation among all competent ministries, government agencies and supervisory authorities. The IAC ensures operational cooperation and coordination of the efforts undertaken by the ministries and government agencies aimed at identifying and mitigating the relevant risks. The IAC is composed of the deputy heads of 20 ministries and government agencies, it is chaired by the Deputy Prosecutor General. To promptly respond to the emerging issues, the IAC Expert Group composed of both experts and senior managers of the competent authorities was established.

256. With a view to increase state authorities' cooperation effectiveness, the National Coordination Council (NCC) chaired by the General Prosecutor of Uzbekistan has been established and operates in the Republic of Uzbekistan. Structurally, the NCC includes the local coordination councils composed of the heads of the government agencies that are responsible for combating crime, the heads of the government authorities and other institutions that are involved in the fight against crime, and also the heads of the crime prevention bodies.

257. Besides that, other interagency anti-crime cooperation and coordination mechanisms have been established and operate in Uzbekistan, in particular:

- National Interagency Commission on Preventing Offences and Combating Crime;
- National Interagency Commission on Crime Prevention among Juveniles;
- National Interagency Commission on Combating Corruption;
- Permanent and temporary investigative teams at the GPO include representatives from the FIU and other LEAs when there is a need to strengthen the fight, detection, and investigation of specific high-risk predicate offences.

258. In the course of the on-site interviews, the law enforcement officers noted close AML/CFT cooperation and coordination at both high and operational levels. The DCEC entered into cooperation and information sharing agreements with more than 20 ministries and government agencies, and the LEAs and FIU have access, including direct access, to a wide range of databases (see IO.6). Analytical materials are exchanged on an ongoing basis via secure communication channels (examples were

demonstrated to the assessment team), which enables to maintain a high enough level of understanding of the current risk and typologies consistent with the NRA findings.

259. The LEAs conduct ongoing analysis of the current situation in the areas they are responsible for and forecast its development in the near term. This information is exchanged via secure communication channels in the framework of interagency cooperation mechanisms and is communicated to the head of the state in form of operational and analytical reports.

260. The FIU regularly meets with the supervisors in the course of round tables, workshops and other training events to share up-to-date information. The assessment team notes the positive effect of regular information exchange between the FIU and the supervisors.

261. The CPF coordination and cooperation are at a sufficient level. The Republic of Uzbekistan has established an effective system of customs and export control, one of the tasks of which is the control of dual-use goods. This work involves the capabilities of the Ministry of Foreign Affairs, the State Customs Committee, Goscomprombek and the Ministry of Investment and Foreign Trade of the Republic of Uzbekistan (see IO.11).

262. As a result of the meetings held and the information provided, the assessment team concluded that the competent authorities actively use the available mechanisms to cooperate and coordinate the implementation of AML/CFT policies, as evidenced by a common understanding of AML/CFT risks and threats, and by demonstrating coordinated measures to mitigate these risks through joint strategic, operational, analytical and other activities.

Private sector's awareness of risks

263. All FIs and DNFBPs showed sufficient awareness of the findings of the NRA as well as of the existing risks. The level of understanding varies depending on the size of the sector. Among FIs, banks, the payment institutions sector, NBCIs, and leasing companies were the most aware, and, to a moderate or sufficient extent, members of commodity exchanges and the postal operator. Of all DNFBPs, the auditors, lawyers and notaries sector showed good awareness of the results of NRAs. The rest of the DNFBPs were less aware.

264. Public bodies use various forms of dissemination and communication of NRA results to the private sector. This includes publishing the publicly available part of the NRA on the website of public bodies.[31] As noted above, the full text of the NRA was shared with the supervisory bodies, which took appropriate steps to inform and explain the results of the NRA to the private sector. In order to disseminate the results of the NRA and ensure its best understanding, meetings and seminars were held with relevant reporting entities in 14 ministries, agencies, prosecutors and PBOs in February 2020.

265. A workshop for the private sector on explaining the results of the NRA and developing necessary measures was held on 11.06.2020 at the GPO Academy using videoconferencing (137 participants).

266. In addition, the DCEC conducts regular training for internal control staff across sectors, including at the Prosecutor General's Academy and the Banking and Finance Academy.

267. Once an NRA has been approved, SRAs are ongoing in almost all sectors, and the private sector is actively involved. Supervisors actively engage with reporting entities by disseminating recommendations, improving NLAs, and conducting training and seminars on ML/TF risk assessment. The findings of NRAs are also communicated to the private sector by supervisors through the issuance of sector-specific ICRs that reflect the relevant risks.

268. The assessors concluded that the country has largely ensured that the findings and conclusions of the NRAs are communicated to the private sector and has taken the necessary steps to raise the awareness of the private sector about the ML/TF risks identified and the measures to mitigate them.

[31] http://new-department.uz/ru/press/news/439/

Overall conclusions on IO.1

269. The Republic of Uzbekistan has made significant efforts to identify, understand and assess its ML/TF risks and develop measures to mitigate them. This work has intensified significantly recently, starting in 2017. The country has been reforming its public authorities and administration, including those involved in the AML/CFT system. Measures are being taken to involve the private sector in AML/CFT activities and raise civil society awareness.
270. The conclusions of the NRA regarding ML risks are reasonable, but the threat level of such categories of predicate crimes as fraud, robbery/theft seems to be underestimated.
271. The country understands the TF risks to a large extent. Still, more attention is needed to identify TF threats and risks within the country and strengthen work with the private sector to prevent possible cases of TF.
272. The assessment of the NPO sector in the NRA was not carried out in sufficient detail, but these shortcomings have been addressed in the SRA.
273. The country has responded to a large extent to the risks identified by changing national policies and coordinating the actions of the competent authorities. At the same time, some of the deficiencies identified in the ML/TF risk analysis have not been addressed. National legislation does not currently contain a definition of national PEPs.
274. The findings of the NRA are used by FIs and DNFBPs to justify the need for enhanced measures in the event of a higher risk situation, based on geographical characteristics, in the client profile and to determine the risk level of the transactions conducted.
275. The aims and objectives of competent authorities are largely consistent with national ML/TF risks. Competent authorities actively use the mechanisms available to cooperate and coordinate the implementation of AML/CFT policies, as demonstrated by a common understanding of AML/CFT risks and threats and by demonstrating coordinated measures to mitigate those risks through joint strategic, operational, analytical and other activities.
276. The country largely ensures that the findings and conclusions of the NRA are communicated to the private sector and takes the necessary steps to raise awareness among the private sector of the ML/TF risks identified and the measures to mitigate them.
277. **The Republic of Uzbekistan is rated as having a substantial level of effectiveness for IO.1.**

CHAPTER 3. LEGAL SYSTEM AND OPERATIONAL ISSUES

Key Findings and Recommended Actions

Key Findings

Immediate Outcome 6

1. All LEAs have access to a wide range of financial information which may be obtained either independently or by contacting the FIU of Uzbekistan – DCEC. DCEC is the central unit of the AML/CFT system of the Republic of Uzbekistan and, with its very wide range of possibilities to promptly receive information from various state bodies and other organizations, provides its own operative units and other LEAs with accurate and quality information to be used in financial investigations. The DCEC has direct access to more than 40 information databases of various public bodies and institutions and uses a large number of STRs from FIs for its financial analysis.
2. A significant level of inter-agency cooperation characterizes the AML/CFT/CPF system in Uzbekistan to obtain financial intelligence, which the FIU provides through proactive information and responses to requests and in the course of joint OIM. Materials of the DCEC are actively used both by their operative units and other LEAs in the detection and investigation of criminal cases on predicate crimes, ML and TF.
3. Most of the information exchange between LEAs and FIUs is between the prosecution authorities and the operational units of the DCEC itself, as these authorities detect and investigate the majority of economic and corruption offences. Other agencies request information when investigating the most significant predicate offences and ML. The exchange of TF information with the MIA and the SSS is also at a high level, and materials are in high demand and effective.
4. The FIU's analysis to large extent supports the operational needs of the LEAs, as evidenced by the fact that over 60 per cent of the submissions were used to initiate a criminal investigation. Ongoing strategic analysis is also in demand by both LEAs and oversight bodies, which use it to communicate typologies to their providers. There are examples of joint detection and supervisory response activities between the FIU and the CB, respectively.
5. FIU and other highly available and actively used financial information by all LEAs on an ongoing basis is mainly used for effective detection and investigation of predicate offences, but to a lesser extent for detecting ML and tracing of proceeds of crime.
6. Both in the course of its own OIMs and at the request of the LEAs, the DCEC applies the powers to suspend transactions in case they are linked to ML/TF/PF or predicate offences. This has a positive impact on the effectiveness of Uzbekistan's AML/CFT/CPF system.
7. All financial and non-financial information received by the DCEC is analysed in a risk-based approach and transmitted to the competent authorities as quickly as possible, not exceeding 5-10 days for high-risk information and 30 days for other information, which increases the speed of information exchange between the FIU and other LEAs and the effectiveness of detecting ML/TF and predicate offences.
8. The DCEC receives most STRs from banks, other FIs provide STRs to a less extent, and DNFBPs (excluding notaries) have never provided STRs or other information. This may harm the availability of financial intelligence to the FIU on indicators of ML/TF and predicate offences identified by reporting entities.
9. All law enforcement representatives noted close cooperation and coordination on ML/TF issues at both a high and operational level. The interaction between the FIU and other competent authorities is carried out exclusively through secure communication channels.

Immediate Outcome 7

1. Any agency involved in OIA, including the DCEC, is authorised to identify and disrupt ML offences in the course of its operation. ML offences may also be identified in the process of pre-investigation checks and preliminary investigations. The decrease in the total number of identified ML offences,

along with the prevailing share of ML identification during the investigations of the predicate offences, and the increase in the number of acquitted persons, indicates insufficient effectiveness of the LEAs efforts to identify and prosecute ML offences. Prosecutors do not make full use of their supervisory powers to influence the quality and effectiveness of the detection and investigation of ML.

2. Not all statistics relevant to the experts' conclusions have been provided; there are discrepancies when comparing statistics from different agencies.
3. The LEAs are focused on priority solving predicate crimes. This is indirectly facilitated by the fact that the MIA has the main competence to investigate ML offences that may decrease the commitment of other LEAs involved in OIA to independently identify ML cases since the detection of ML offences is not part of the assessment of their activity results.
4. Most ML cases identified in Uzbekistan are related to self-laundering and do not involve complex ML schemes (most frequently criminal proceeds were laundered by way of purchase of movable and immovable property and its registration in the name of third parties acted as nominee owners). Only few persons were prosecuted and convicted for third-party ML, and only few instances that involved the laundering of proceeds of criminal offences committed abroad were detected.
5. Overall, the competent authorities now have sufficient powers and access to electronic databases that enable them to gather financial intelligence for identifying and investigating ML cases. The joint regulation governing the procedure, objectives and scope of (parallel) financial investigations was adopted only in May 2021. There was no methodology and practice for such investigations prior to the adoption of the aforementioned regulation, which affected the overall quality of identification and investigation of ML cases.
6. The Uzbek authorities pay significant attention to training, re-training and professional development training of officers of LEAs and other government agencies involved in the AML/CFT. There are sufficient resources (human, material, information, technical and methodological) for successful identification and criminal prosecution of predicate offences in general and ML in particular.
7. The identified and investigated ML typologies, schemes and techniques are in common consistent with the national threats and risks and the national AML policies. The exception to this are the third-party ML (including professional ML), and laundering of proceeds of fraud and embezzlement, which are underestimated.
8. The country's judiciary demonstrates a commitment to integrity and impartiality in adjudicating ML cases and passing sentences, both where acquittals are necessary and where there are grounds for conviction, which is one of the defined objectives of judicial reform and judicial independence.
9. Sanctions for ML offences provided for in the legislation are dissuasive, but not proportionate and, therefore, the courts impose more lenient sentences and punishments on a large number of convicts. Sanctions are not imposed on legal entities involved in ML.
10. Convictions for predicate offences are used as the alternative measures of criminal prosecution for ML. The presented information did not allow for making a definite conclusion about the application of other alternative measures.

Immediate Outcome 8

1. According to specifics of legal regulation, confiscation is not considered in Uzbekistan as the main goal and mechanism of implementation of the state policy in the fight against crime in general and AML/CFT in particular.
2. The priority application of confiscation is compensation for material damage (restitution to victims). Confiscation of criminal proceeds applies only when there are no grounds for restitution.
3. Confiscation is based solely on criminal procedural mechanisms. Non-conviction based confiscation is applied in cases limited by the country's law.
4. In the process of criminal proceedings and prosecutions, the LEAs use the procedural powers vested in them to seize property that is the proceeds of crime and instrumentalities used for committing

crimes as the provisional measure for securing further compensation of inflicted material losses and confiscation of property.

5. However, recovery of inflicted losses and confiscation of criminal proceeds are, to a large extent, achieved not through the efforts of the LEAs. Instead, in most cases, guilty persons voluntary surrender property obtained by them through crime in exchange of release from criminal liability or mitigation of punishment as provided for in the criminal legislation. The perpetrators are voluntarily compensated for a large part of the damage (criminal proceeds).
6. Uzbek authorities provided statistics on the seizure of property by LEAs, confiscation of property by courts, enforcement of court orders and actual appropriation of confiscated property to the state budget. However, lack of comparable data about the number of convictions for predicate offences that entailed confiscation, the value of confiscated assets and some other relevant information did not allow assessors to arrive at a definite conclusion about the effectiveness of measures taken by the country.
7. Monitoring of cross-border movement of cash is carried out in Uzbekistan in a comprehensive and systematic manner. Confiscation of undeclared (falsely declared) cross-border movement of currency as well as instruments of customs crimes is applied in the country and is an effective, proportionate and dissuasive sanction.
8. The decrease in the number of executed court orders regarding appropriation of (confiscated) property to the state's revenue was noted by assessors as a negative trend.

Recommended Actions

Immediate Outcome 6

1. The MIA, the SSS, and the SCC should make greater use of FIU resources in conducting parallel financial investigations, identifying ML and tracing the proceeds of crime, especially for corruption offences, for further confiscation. Joint OIMs, which are effective in detecting predicate offences, should also be used to identify ML.
2. Given that the basis for the FIU's analysis is STRs, there is a need to increase interaction with supervisors and the private sector to improve the quality and quantity of STRs provided, especially concerning the information provided by DNFBPs.
3. The DCEC needs to increase the amount of proactive analysis and spontaneous dissemination to the LEAs, as well as a greater focus on tracing criminal proceeds.

Immediate Outcome 7

1. Uzbekistan should take additional measures for improving the effectiveness of ML identification, disruption and prosecution by the LEAs. The fight against ML should be identified as the priority. It is also necessary to increase efforts to identify complex ML, ML by third parties (including professional laundering). Uzbekistan should revise (and adopt the relevant laws, if necessary) the practice to enable criminal prosecution for ML irrespective of criminal prosecution for predicate offences.
2. Uzbekistan should take measures to establish the administrative liability of legal persons for ML, to broaden the range of effective, proportionate and dissuasive sanctions against legal persons for violating ML/TF legislation.
3. In order to ensure the effectiveness and proportionality of sanctions Uzbekistan should establish in the criminal law a gradation of punishment for ML offences depending on the amount of money laundered. It is also necessary to establish stricter liability for ML offences committed by special actors (for example, officials, persons previously convicted of ML, as part of an organised group).
4. Uzbekistan should extend the international cooperation, inter alia, for identification and criminal prosecution for ML related to laundering proceeds of foreign predicate offences as well as for ML committed abroad.
5. The GPO should more effectively supervise the legitimacy of activities of the preliminary investigation authorities and agencies involved in OIA.

6. Uzbekistan should more effectively gather and maintain the AML statistics.
7. Competent authorities of Uzbekistan should ensure more effective conducting of (parallel) financial investigations, and a unified practice of such investigations in line with the adopted joint regulation.

Immediate Outcome 8

1. Uzbekistan should amend its legislation: to establish confiscation as an institution of criminal law (as a legal consequence of committed predicate, ML, and TF offences); to supplement the Criminal Procedural Law with a norm obliging criminal prosecution bodies to prove the criminality of the property, as well as a norm giving the superior court the authority to apply confiscation when reviewing the conviction.
2. Uzbekistan should consider establishing an increase in the practice of non-conviction based confiscation as well as possible confiscation of unconfirmed proceeds as a form of non-conviction based confiscation.
3. Uzbekistan should continue the work for more extensive application of provisional measures to ensure compensation of inflicted losses as well as for identification, seizure, confiscation and recovery of criminal assets moved to foreign jurisdictions.
4. Given that the importation of foreign currency cash prevails over its exportation, Uzbekistan is recommended to intensify efforts to identify instances of illegal import of currency cash intended, inter alia, for further use for ML/TF purposes in the country.
5. Uzbekistan should take additional measures to improve the effectiveness of enforcement of court orders related to compensation of inflicted losses and actual appropriation of confiscated property to the state's revenue.
6. Comprehensive and reliable statistics should be maintained regarding property confiscation and restitution to victims.

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

Immediate Outcome 6 (Financial Intelligence ML/TF)

Use of financial intelligence and other information

279. In the process of investigation of predicate offence and ML/TF, all LEAs of the Republic of Uzbekistan, including the SSS, the MIA, the SCC, the GPO and the DCEC, have access to a wide range of financial intelligence sources. Financial investigations are conducted through OIM (including joint investigations and proceedings), financial analysis, collection of information using different information resources (including the interagency electronic information exchange system), and use of various publicly accessible and internal information sources, such as:
    - Information held by the DCEC and provided upon request, including information on STRs filed by financial institutions and DNFBPs;
    - Databases containing information of persons who have been held criminally or administratively liable;
    - Tax information, and information held in the registers of legal entities and individual entrepreneurs;
    - Customs information, and information on purchased railway and airline tickets;
    - Information on ID documents, registration records and records of births, deaths and marriages;
    - Information contained in commercial databases.
280. The LEAs also receive information from their foreign counterparts via the Interpol channels and other operational cooperation frameworks as well as under the mutual legal assistance agreements.

281. In the process of OIA, the LEAs obtain required information and documents from companies, institutions and organizations at the requests of inquiry officers, investigators, prosecutors and courts. Forced seizure of documents is also used in the process of conducting searches during the preliminary investigations.

282. LEAs and courts receive information on transactions, accounts and deposits constituting bank secrets on the basis of Law "On the bank secrecy".

283. Uzbekistan has established the special LEA under the GPO that is responsible for OIA and inquiries into economic and corruption-related offences as well as into ML and predicate offences – the DCEC, which is at the same time the national FIU. The total number of employees is over 1000.

284. The DCEC is authorized to initiate criminal proceedings and conduct inquiries into economic crimes. The DCEC conducts a comprehensive analysis of the national efforts aimed at combating economic crimes, corruption and ML/TF/PF and also identifies instances of embezzlement and misappropriation of the state budget funds, that is largely responsible for its leading position in detecting ML cases and predicate offences.

285. Since the DCEC is a law enforcement type of FIU, its structure includes both operational units, which conduct OIA, inquiries and financial audits, and analytical units, whose responsibilities include analysis of STRs and other information received from FIUs and DNFBPs. The analytical unit transmits the results of financial investigations to operational units and other LEAs.

286. When conducting financial investigations, the DCEC also uses a wide range of other financial and non-financial information available through automated access to 44 databases maintained by different ministries and government agencies. Besides that, the DCEC uses information obtained in the framework of international cooperation and from open sources (social media, messaging services, commercial databases). In order to collect the required information, the DCEC uses online automated access to various databases through the secured E-XAT and LOTUS platforms that are also connected to different organizations, FIs and DNFBPs.

287. The DCEC accesses most databases online in automatic mode. Where necessary, the DCEC also automatically sends requests for additional information to FIs and DNFBPs. The key databases of the government agencies and institutions accessible by the DCEC are presented in the table below.

Table 6.1: Databases of Government Agencies and Institutions Accessible by DCEC

№	Agency/ Institution	Provided Information
1.	Cadastre Agency under the State Tax Committee of the Republic of Uzbekistan	- Tashkent real estate property register; - Regional real estate property registers
2.	Ministry of Employment and Labor Relations	- Register of foreign citizens licensed to work in Uzbekistan; - Register of Uzbek labor migrants
3.	State Customs Committee (a total of 20 databases)	- Bank accounts of taxpayers; - Register of legal persons; - Additional income declarations; - Foreign currency account receivables; - Information on invoices issued/ received by business entities; - Payment reports; - Treasury (budget, etc.); - Collection orders; - Analysis and processing of information on activities of business entities; - Database of state tax inspectorates (individual pension savings accounts); - Bank account statements; - Account reconciliation statements of business entities; - Tax payment history (legal and natural persons); - Tax overpayment statements, etc.
4.	Ministry for Information & Communication Technology Development	- Register of national information resources and information systems of government authorities; - Register of issued licenses to construct and operate telecommunication networks and provide telecommunication services.
5.	Public Services Agency under the	- Single state register of companies and organizations.

	Ministry of Justice of the Republic	
6.	Ministry of Justice	- Register of associations of legal entities; - List of representative offices and branches of international non-government non-profit organizations; - Register of religious organizations, etc.
7.	Interior Ministry (a total of 14 bases);	- Civil biometric passports; - Criminal record information center; - Information on change of residence and registration; - Death certificates; - Administrative offences; - Register of transport vehicles; - Wanted lists; - Register of weapons held by Uzbek citizens and organizations, etc..
8.	People's Bank (joint-stock commercial bank)	- Database of individual pension savings accounts
9.	State Customs Committee	- Information on cargo customs declarations; - Information on passenger customs declarations.
10.	Central Bank	- National bank depositors database (information on business entities and their accounts opened with the Uzbek banks).
11.	Finance Ministry	- State budget-funded (government-funded) organizations and their current accounts; - Management reports and financial statements; - Interagency cooperation
12.	Regional Electric Power Grids (joint-stock company)	– Accounts receivable and payable by electric power consumers
13.	O'zsuvta'minot (joint-stock company)	– Accounts receivable and payable by potable water consumers
14.	Uztransgas (joint-stock company)	- Location of gas points; - Monitoring of gas consumption; - Balance of received and distributed gas
15.	Hududgazta'minot (joint-stock company)	– Accounts receivable and payable by natural gas consumers
16.	Ministry of Housing and Public Utilities	– Accounts receivable and payable by utilities consumers

288. The DCEC is the core of the functioning of the national AML/CFT system of Uzbekistan. It has all the necessary capabilities and resources that enable it to conduct high quality strategic analysis for combating ML/TF and predicate offences and to disseminate high quality information and materials to other competent authorities.

289. Based on the existing cooperation agreements, the LEAs, if necessary[32], request financial intelligence from the DCEC in the process of financial investigations and investigations into predicate offences and TF. The DCEC, in turn, responds to the incoming requests and also spontaneously disseminates financial analysis to the LEAs.

290. For example, when investigating ML, the OIA units of the DCEC used FIU information in 63% of criminal cases (128 out of 201), other LEAs were less active: the SSS - 26% (5 out of 19), the MIA - 11% (5 out of 47). In terms of TF, the SSS used the DCEC's materials in 5 out of 28 (17%) criminal cases, and the MIA in 9 out of 17 (53%). These statistics show that the results of financial investigations to a large extent assist in the detection and investigation of criminal cases, which demonstrates the high quality of the DCEC's materials, as well as the availability of financial intelligence provided by the FIU to other LEAs.

291. All LEAs have ample opportunities to obtain relevant financial intelligence on their own, including bank secrecy, directly from financial institutions following the initiation of criminal cases and, from June 2021, within the framework of the OIA.[33]

[32] Where the LEAs does not have independent operational access to such information.
[33] Law No.ZRU-697 on Amendments and Modifications into Certain Legislative Acts of the Republic of Uzbekistan dated 28.06.2021.

292. The powers of the DCEC allow the collection and transfer of data containing banking and other legally protected secrets. Also, the DCEC may request any additional required information from reporting entities when carrying out analytical work, regardless of whether such entity has sent an STR or not. No records of such requests are kept due to the fact that in this format, the information is requested on an ongoing basis in an automated mode through electronic communication channels. The examples of successful implementation of the materials provided by the DCEC fully support this statement. Moreover, the analysis of the examples of responses to LEAs and the demonstrated briefing notes prepared on the work results on LEAs' requests indicate that the LEAs' analysts make extensive use of this authority.

293. As seen from the statistics, the bulk of the information exchange between the LEAs and FIU is between the prosecution authorities and the operational units of the DCEC itself. This is due to the fact that it is the prosecution authorities and DCEC units that detect and investigate the majority of economic and corruption offences. For example, the prosecution authorities investigated 1,401 crimes (of which 1,333 were initiated) between 2016 and 2020. 1,401 (of which 1,333 were initiated by the DCEC) tax crimes, including trade violations, representing over 99% of the detected crimes in this category in the country and 86% of corruption-related crimes (16,919 out of 19,675). According to the NRA, these categories of crime are characterised by the highest amount of criminal proceeds. MIA agencies investigate crimes characterised by comparatively small criminal proceeds (illegal drug trafficking, fraud, theft), while SSS, on the contrary, investigate the most significant and essential cases, but in small numbers.

Table 6.2: Statistics on ML and predicate crimes Information Sharing between DCEC and LEAs

LEAs	2016		2017		2018		2019		2020	
	Spontaneously	At request	Spontaneously	At request	Spontaneously	At request	Spontaneously	At request	Spontaneously	At request[34]
GPO		436		285		283		235		105
SSS		25		5		0		7	4	34
MIA		15		14		4	1	21	3	27
SCC							1	4	1	3
DCEC units	72	343	122	361	161	419	512	431	1,491	188
TOTAL	891		787		867		1,211		1,856	

294. Practices of conducting joint operational activities and establishing joint investigation teams are widely used, within which financial information and intelligence are exchanged routinely without the need for special requests. Such practices are quite commonly used as a mechanism of cooperation with all LEAs. Provided statistics definitely indicate the effectiveness of such cooperation, as 96% of joint operational activities resulted in the initiation of criminal proceedings, including ML-related criminal proceedings.

295. In 2016-2020, the prosecution authorities set up 366 (of a total of 957) joint investigative teams to investigate multi-episode and particularly complex criminal cases, which involved officers of the DCEC (see Case study 7.7). In addition to participation in inter-agency investigative teams, the FIU interacts with the investigative units of the LEAs as part of the execution of individual instructions from criminal investigators (no statistics are kept due to the enormous number of instructions sent).

Table 6.3: Statistics on Joint Operational Activities

LEAs	Number of joint OIMs	Number of identified criminal cases	Number of identified ML cases
MIA	1,985	1,844	0

[34] In the context of COVID-19 related epidemiological situation, the investigations were conducted in a limited scope due to the imposed restrictive measures. After the pandemic-related restrictive measures were relaxed, the investigations were resumed in full scope, which led to a significant increase in the number of incoming information requests. For example, 105 requests were received from other LEAs and 116 requests were received from the DCEC operational units in January-April 2021.

SSS	2,257	2,218	5
SCC	65	46	0

Case Study 6.1

Based on the analysis of the incoming STRs related to two affiliated LLC beneficially owned by individual A., the DCEC identified the following indicators of illegal financial activities:

- Discrepancies in the accounting documents related to purchased and sold goods (cashing out and fictitious sale transactions);
- Unlicensed business operations involving the provision of road transportation services which yielded exceptionally large income (UZS 1.4 billion);
- Provision of construction, assembly and other services within a short period of time without necessary material, technical and labour resources;
- Evasion of taxes in amount preliminary estimated at UZS 8.7 billion.

In parallel, numerous STRs were received indicating conversion of funds into foreign currency.

The following information sources were used in the process of analysis:

- STR databases and additional information requested from financial institutions;
- Open information sources (Ministry of Transport of Uzbekistan);
- Databases of the STC (tax returns and information on other existing companies), the MIA (criminal records) and the national database of bank depositors (NDBBD, banks with which accounts have been opened).

The results had been disseminated to the DCEC operational units where they were verified with the OIA. It was also established that A. obtained criminal proceeds in the amount of UZS 741 million by carrying out illegal financial transactions and converted these funds into foreign currency in the amount of USD 70 thousand for giving the appearance of legitimate origin of the illegally obtained money.

Furthermore, the gathered criminal intelligence also revealed that the executive officer of the bank that provided services to LLCs failed to timely execute the collection order issued by the state tax inspectorate for recovering the unpaid taxes.

As a consequence, more than UZS 1.6 billion was transferred from the accounts of the aforementioned companies to accounts of other companies in exchange for the high-priced goods that were further sold for cash.

Based on the gathered criminal intelligence and the findings of the conducted pre-investigation checks, criminal proceedings were launched against A. under the CC Art.179 (fictitious business), Art.184 (tax evasion), Art.189 (breach of trading regulations), Art.190 (unlicensed business activities) and Art.243 (ML) and also against the executive officer of the bank under Art.207 (neglect of official duties), and case materials were submitted to the prosecution office.

The conducted criminal investigation proved the identified facts, and criminal charges were brought against the suspects.

Case Study 6.2

In the course of criminal intelligence gathering and pre-investigation check into potential fraud and illegal raising of funds (or) other assets initiated jointly by the DCEC and the MIA, the DCEC conducted the financial investigation.

The parallel financial investigation conducted by the DCEC revealed the following:

- More than five identified retail outlets were used for:
  - Soliciting funds from unsuspected people by way of selling tickets that allegedly granted the right to buy cars for the originally invested funds (the amount of funds raised in such manner was estimated at UZS 2 to 10 million);
  - Collecting the cash revenues and depositing them into different branches of the banks to gain full trust and confidence;
  - Pursuing an aggressive advertising campaign.

- Transferring funds under fake interest free loan agreements to the accounts of auto shops for purchasing expensive luxury cars.
- Placing the working funds into the shadow economy by cashing out UZS 2 billion from the bank.
- Investing criminal proceeds in the amount of UZS 6 billion into deposit accounts of newly established business entities as a contribution to their authorized capital.

The following information sources were used in the process of analysis:

- STR databases and additional information requested from financial institutions;
- Open information sources (existence of 5 retail outlets);
- Databases of the STC (tax returns), the MIA (criminal records) and the NDBBD (banks with which accounts have been opened).

The analytical report prepared based on the outcomes of the examination of the aforementioned information was disseminated to the MIA.

Upon receipt of the report, the MIA initiated criminal proceedings under Art.168 (fraud), Art.188-1 (illegal raising of funds and (or) other assets) and Art.243 (ML) of the CC.

296. In view of the common practice of joint OIMs and other cooperation formats, the assessors concluded that all LEAs had access to financial intelligence, which is effectively used in the country for identifying and investigating economic crimes and TF.

297. Upon detection of TF suspicious indicators, the relevant information is disseminated to the SSS and MIA that are the key agencies responsible for identification and investigation into criminal offences related to terrorism and TF. The analysis findings are provided to the LEAs both spontaneously and at the request of the competent authorities. In the course of the investigation into terrorism-related criminal offences, the SSS and the MIA use the FIU capabilities to examine the financial aspects of committed crimes and to identify terrorist financing sources. This information is demanded and the intensity of information exchange in this sphere has increased in recent years as evidenced by the more active use of information provided by the DCEC for an investigation into terrorism and TF-related criminal cases. The statistics of information exchange on TF are in line with the efforts of LEAs to detect and investigate these crimes in the Republic of Uzbekistan (see IO.9).

Table 6.4: Statistics on TF Information Sharing between DCEC and LEAs

LEAs	2016		2017		2018		2019		2020	
	Spontaneously	At require	Spontaneously	At require	Spontaneously	At request	Spontaneously	At request	Spontaneously	At require
SSS	99	91	98	129	126	133	167	86	199	184
MIA	36	4	2	4	6	17	9	21	6	15
Total	135	95	100	133	132	150	176	107	205	199

298. Besides that, the competent authorities are engaged in regional programs aimed at identifying persons associated with activities of international terrorist organizations and their cells. In particular, the DCEC is involved, in cooperation with the LEAs and financial institutions, in the ongoing “Barrier” operation which is aimed at the identification of international terrorist centers, terrorist cells and their accomplices, primarily terrorist fighters operating in parts of Syria and Iraq controlled by the ISIL international terrorist organization.

299. All LEAs are aware of the FIU’s capability to promptly obtain meaningful information from abroad and use it in practice. In 2016-2020, 73% of ML-related information requests were initiated by the SSS, the MIA and investigation units of the GPO, while the remaining 27% of requests were initiated by the DCEC OIA units. These statistics show that the FIU capabilities are well understood and used by the LEAs and the DCEC OIA units.

300. Despite the FIU's significant contribution to the detection of ML in the country and the focus on the use of financial information for ML detection by the operational units of the DCEC, it appears that other LEAs pay less attention to the need to identify ML when investigating predicate offences. Thus, as a result of over 4,300 joint operations and over 4,100 criminal investigations into predicate

offences, where FIU information was used, only 5 cases of ML were detected. The conclusion is also confirmed by the fact that enquiries to the FIU from the SSB, the MIA and the SCC, sent in a country-specific manner on substantial and significant criminal cases, despite the quality of the information provided by the FIU, served as grounds for launching only five criminal proceedings for ML on the part of the SSS.

301. Information exchange between the FIU and the LEAs in the field of CTF is at a consistently high level and correlates with the number of crimes detected in this area.

302. The AML/CFT system of the Republic of Uzbekistan is characterised by a high degree of availability of financial intelligence to all competent authorities. A wide range of financial and non-financial intelligence is available to all LEAs and can be obtained independently or through requests to the FIU. Financial information with bank secrecy is available to all LEAs, particularly under legally defined circumstances, during the OIA stage. The FIU itself, as evidenced by the statistics, actively processes the information received and passes it on to its OIA units and other LEAs for further consideration. The quality of materials is high, as evidenced by the fact that a significant part of the criminal proceedings initiated in the country for ML occurs with the use of materials of the DCEC. The practice of joint investigative teams demonstrates high efficiency in detecting predicate crimes.

STRs and other information received and requested by competent authorities

303. The DCEC receives STRs, including attempted transaction reports, from entities engaged in transactions with funds or other assets in the prescribed manner not later than one business day following identification of such transactions. In 2016-2020, the DCEC received on average around 1,100 STRs every day. The suspicious transaction reports are subdivided into two categories: (1) reports related to transactions that meet the established suspicious criteria (set out in the internal control rules of reporting entities); and (2) reports related to other transactions that do not meet the established criteria, but suspected by reporting entities of being linked to ML/TF (i.e. proper STRs).

Table 6.5: Statistics on Information Sharing between DCEC and Reporting Entities

Types of institutions	2016		2017		2018		2019		2020	
	Criteria-based reports	STRs	Criteria-based reports	STRs	Criteria-based reports	STRs	Criteria-based reports	STRs	Criteria-based reports	STRs
FIs	33,577	191,857	64,222	171,884	110,331	134,902	283,037	99,631	564,751	133,872
DNFBPs	-	-	-	-	2	-	2	-	-	-
Total	225,434		236,106		245,315		382,670		698,623	

304. The bulk of the information is received by the DCEC from credit institutions. To a less extent, STRs and other reports are filed by the securities market participants, the exchange members, payment institutions and NBCI. Other FIs (insurance and leasing institutions, postal operator) provide information rarely. There were no reports from the DNFBP sectors (except notaries), which is the deficiency in financial intelligence information on ML/TF indicators identified by the reporting entities available to the DCEC.

305. The statistics demonstrate certain trends toward a reduction in the number of non-criteria based reports and an increase in the number of reports that meet the established criteria as a result of the ongoing awareness raising and outreach work conducted by the DCEC and supervisors among the reporting entities to improve quality of incoming reports.

306. The decline in the number of incoming non-criteria based reports may be considered a positive trend, since the FIU officers have told the assessors that sometimes credit institutions file “defensive” STRs, and the DCEC is taking measures to eliminate such defensive reporting. The increase in the number of criteria-based reports is partly associated with the participation of Uzbekistan in the project initiated by the CH FIU for identifying TF channels, and, therefore, money transfers to/ from regions with increased terrorist activities meet the mandatory reporting criteria.

307. Transactions are necessarily reported to the DCEC if any party to such transactions is:

- A person who resides, stays or is registered in a country that does not participate in AML/CFT/CPF cooperation;
- A legal or natural person who is involved or suspected of being involved in terrorist activities or in WMD proliferation;
- A legal or natural person who, directly or indirectly, owns or controls an entity that is involved or suspected of being involved in terrorist activities or in WMD proliferation;
- A legal entity that is owned or controlled by a natural person or an organization that are involved or suspected of being involved in terrorist activities or in WMD proliferation.

308. The number of STRs received on topics possibly related to TF is constantly increasing. The sharp increase in the number of reports in 2019 and 2020 is related to the strengthening of work with reporting entities, as well as the accession of the Republic of Uzbekistan to the CIS CHFIU and the implementation of Operation Barrier, which started to receive reports on operations related to high-risk areas for terrorist financing, as well as operations of persons on the CIS ATC lists. The increase in the number of reports correlates with an increase in initiative reporting by the FIU through TF (Table 6.4), which demonstrates the effectiveness of the ongoing work in this area. All of the reports selected for analysis were examined as a matter of priority.

Table 6.6. Statistics of regarded STRs with TF risk.

2016	2017	2018	2019	2020
68	79	136	685	1419

309. The DCEC has direct access to a wide range of financial and non-financial information obtained through the electronic document management system. Financial investigations use all data from the available databases mentioned in the core issue. 6.1.

310. Customs authorities provide information on illegal imports and exports of national and foreign currency in cash to the DCEC. Interaction on the exchange of information obtained as a result of declarations between the DCEC and SCC is regulated by an interagency agreement on cooperation, as well as a joint Regulation on the Procedure of Interaction. On the basis of these interdepartmental acts, the DCEC has online access to the SCC databases (information on PCDs and CCDs).

Case Study 6.3

The SCC is continuously analysing information received under the international Operation Gamma.
According to the information received, 3 persons from the same region brought into the country foreign currency in large amounts (each of them had about 50 thousand USD).
In particular, citizen "Ahmed" was carrying over 50 thousand USD. In particular, citizen "Ahmed" had over 50,000 USD, "Akbar" over 60,000 EUR and "Akmal" over 45,000 EUR.
During a brief discussion with the two men, customs officials were able to establish that they were

- are engaged in labour assembly and repair work in the Republic of Finland, in "Work with us" and "Trust us" companies;
- employed about 750-800 Uzbek nationals in this company;
- the money imported was the earnings of fellow villagers who their relatives brought in.

The SCC sent this information to the DCEC for examination, during which the DCEC sent an international request to the FIU of Finland. The information collected from the Finnish FIU and the DCEC's territorial office established that:

- the persons in question are in fact carrying out their work in Finland, as they are listed in the database of natural persons carrying out work in a foreign country;
- there is no criminal record regarding their residence and workplace;
- the imported funds do not have a criminal origin.

For reference: Operation Gamma aims to prevent smuggling and violating customs laws in the channels of international passenger transportation by air.
According to the operation plan, in the course of the activities, proactive data on suspicious movements

is exchanged between the customs services of the CIS countries and checks are initiated to cross possible offences.

311. Most spontaneous disseminations provided by the FIU contain information received from financial institutions. When drafting spontaneous dissemination or an answer to a request, the FIU uses STRs as the basic information to determine whether or not it is necessary to request additional information not only from reporting entities but also from the government authorities within their purview.

Table 6.7: Statistics on Use of STRs for Preparing ML-Related Disseminations to LEAs

	Number of received requests	Number of incoming requests analyzed with the use of STRs	Total number of STRs used for analyzing incoming requests	Number of spontaneous disseminations	Number of spontaneous disseminations drafted based on STRs	Number of STRs used for drafting spontaneous disseminations
2016	819	687 (83.8%)	28665	72	62 (86.11%)	7556
2017	665	518 (77.8%)	25935	122	102 (83.6%)	9779
2018	706	571 (80.8%)	26122	161	122 (75.7%)	12117
2019	698	586 (83.9%)	32108	512	486 (94.9%)	33489
2020	357	296 (82.9%)	19992	1491	1455 (97.5%)	86604

312. In 2016-2020, a total of 280 thousand incoming STRs were used for drafting analytical materials for dissemination to the DCEC operational units and other LEAs. STRs were used in more than 80% of answers to the received requests, and in more than 90% (especially after 2019) of spontaneous disseminations. The statistics show that STRs are an important element of the analysis conducted by the FIU and are effectively used for preparing both answers to requests and spontaneous disseminations.

313. STRs are prepared with the use of the special software (MONEYOPERATION) that has been developed by the DCEC and provided free of charge to all entities engaged in transactions with funds or other assets, and personnel of reporting entities receive training in the use of this software. The use of specialized software eliminates technical errors when filling out and processing incoming STRs.

314. The DCEC has arranged for the automated control of all incoming STRs on a daily basis. About 50 algorithms have been developed that enable automatically identify of errors in incoming reports and assess information contained in the STR standard forms at different stages of their processing. If an incoming STR contains distorted, erroneous or duplicate information, the reporting entity that has filed such STR is instructed to eliminate the identified errors and repeatedly send the corrected STR to the DCEC within one business day following its rejection. On average, about 1.5% of STRs received by the DCEC require correction.

315. STRs are categorized into groups based on the types of financial transactions, such as money transfers; depositing funds to plastic cards; transfer of funds under commercial agreements; purchase and sale of foreign currency cash; withdrawal of cash from plastic cards.

Table 6.8: STR Statistics

#	TYPES OF FINANCIAL TRANSACTIONS	2016-2020		
		STRs	Amount (bln)	Percentage
1	Money transfers	902,061	36,132	7%
2	Deposits to plastic cards	61,470	9,985	2%
3	Payments under contracts	440,171	449,138	83%
4	Purchase and sale of foreign currency	139,382	32,461	6%
5	Withdrawal of cash from plastic cards	245,061	16,548	3%
TOTAL		1,788,145	544,265	100%

316. The presented statistics show that transactions involving the transfer of funds under various contracts/agreements are primarily identified by banks as suspicious. This conclusion is indirectly

supported by the NRA which identifies violations of the trade and service provision regulations as posing a very high risk.

317. In general, these criteria provide for the initial categorization of the incoming reports. Then, the received STRs are further categorized based on types of persons (designated persons included in the Lists; persons, information on whom is requested by the LEAs; persons, information on whom is requested by foreign authorities; persons put on a wanted list; persons who are subject to monitoring; and persons who meet the criteria (indicators) related to geographic location, frequency of transactions, typologies, FI location, etc.).

318. After that, the initially processed STRs are uploaded into the information system where they are recorded, processed and reviewed for further use in the course of analysis.

319. The incoming reports are distributed to particular analysts who identify and obtain necessary additional information using the available databases or requesting data from reporting entities, government agencies or foreign partners, and conduct the analysis.

320. Since the DCEC receives a large number of STRs, the incoming reports are prioritized for further analysis. The assessors have reviewed the STR prioritization criteria (approved by the DCEC internal regulation) and agree that these criteria are relevant and consistent with the identified ML/TF/PF risks.

321. Although the Uzbek competent authorities believe that there are no significant PF threats in the country, the DCEC receives and analyzes PF-related reports filed by credit institutions. In 2016-2020, the DCEC received from financial institutions 1,784 reports concerning transactions amounting in total to USD 39.6 million, EURO 6.0 million, UZS 3.6 billion and RUR 576.1 million.

Table 6.9: Statistics on PF-Related STRs Filed by FIs

Number of reports filed by FIs	2016	2017	2018	2019	2020	Total
	288	240	278	394	584	1,784

322. Most reported transactions involve payments of wages and dividends to employees and founders who are citizens of the Islamic Republic of Iran. This transaction flow reported to the DCEC and the work conducted y by the country (see IO.11) support the conclusions of the competent authorities. Since the national PF risk assessment has not been conducted in Uzbekistan yet (which is not a deficiency in terms of the FATF standards), this work may be assessed very positively as it contributes to the ongoing monitoring and identification of risks in this area.

323. Since 2018, the DCEC is authorized to independently suspend transactions carried out through accounts for a period of up to 30 days, if there are sufficient reasons for doing this, which may be related to the identified predicate offences or ML/TF/PF cases. A transaction suspension order may be issued based on the reported cases or at the request of the LEAs or the DCEC operational units or at the request of foreign competent authorities. It should be noted that these powers of the DCEC have a positive impact on the effectiveness of the AML/CFT/CPF measures implemented in Uzbekistan. The statistics show that the DCEC more actively uses these powers every year, especially based on the STR analysis outcomes. These powers also strengthen and extend the DCEC ability to secure funds obtained by suspects through crime.

Table 6.10: Statistics on ML Transaction Suspension Orders

Year	Number of Entities	Amount of Suspended (Frozen) Funds (USD)	Suspension Grounds	
			STR	LEA Request
2018	12	2,181,343	8	4
2019	14	1,450,490	12	2
2020	22	1,984,959	10	12
2021	45	3,104,781	32	13

324. The powers of the DCEC allow the collection and transfer of data containing banking and other secrets protected by law. The DCEC may request any additional information required from reporting entities when conducting analytical work, regardless of whether such entity has sent an STR or not. The records of such requests are not kept due to the fact that in this format the information is requested on a continuous basis in an automated mode via electronic communication channels. The examples of successful implementation of materials, given by the DCEC, fully confirm this statement.

325. When preparing analytical materials for dissemination to the operational units and LEAs, the Uzbek FIU actively uses information provided by financial institutions and also freezes funds, based on the received STRs, for ensuring their security. Information on STRs filed by financial institutions, along with additional information requested from relevant agencies and organizations, is accessible for and can be promptly obtained by all interested law enforcement agencies. STRs were used in most disseminations forwarded both at the request and spontaneously. In view of the number of incoming STRs, the risk-based approach applied by the DCEC for processing the received reports and also a wide range of other information available to the DCEC which can obtain it directly from the information holders, it can be stated that the FIU provides high quality analysis to the LEAs and itself uses these analytical materials in the process of OIM within its purview. The interviewed LEA officers also noted high quality and completeness of disseminations received from the DCEC.

Case Study 6.4

Following examination and analysis of the incoming STRs, the DCEC identified the facts of tax evasion and violation of the trade regulations on an exceptionally large scale.

In particular, within a short period of time (3 months), the Importer company imported various goods worth over USD 30 million, but declared much smaller sale revenues and used part of them only for payment of customs duties and fees.

It was also found out that the imported goods were removed by third parties who were unaffiliated with the Importer company and acted based on the powers of attorney issued by Importer company.

When it was time to submit the quarterly tax statement, the executive officers terminated all activities and dissolved the Importer company and, thus, evaded payment of the relevant taxes.

Besides that, the DCEC received another STR indicating that the shadow managers of the Importer company registered a new company – Volunteer Company in the name of another front person and launched further illegal activities.

It was also found out that the Importer company and Volunteer company were registered at the same legal address and dealt with the same counterparties.

The executive officers of Volunteer company applied for the conversion of funds into foreign currency to be further transferred to foreign Company Limited registered in the offshore zone.

The DCEC took measures to suspend the transaction (USD 497 thousand) for 30 business days and forwarded the request to the FIU of the foreign country in which the accounts of the offshore company were registered.

According to the information received from the foreign FIU, the beneficiary of Company Limited was the individual called Akhmadbai who acted as the shadow director of both Importer company and Volunteer company.

Further investigation revealed that Akhmadbai provided the “intermediary services” by issuing customs declarations for goods imported by other parties to the shell companies established by him with the purpose of concealing actual sales revenues and evasion of taxes.

In exchange for these “services”, he charged the fee in the amount of 1 to 3 percent of the cost of the cleared imported goods.

In the course of financial investigation and OIMs, it was established that Akhmadbai, acting through the nominee executive officers, contributed cash obtained as a result of these illegal activities to the authorized capital of Volunteer company.

During the interrogation, Akhmadbai confessed that he was the beneficiary of Company Limited and that the funds that he planned to transfer to this company were intended for paying for real estate property in Dubai.

Based on these findings, criminal proceedings were initiated against the shadow director and executive

officers of Importer company and Volunteer company under Article 179 (fictitious business), Article 184 (tax evasion), Article 189 (violation of trade and service provision regulations) and Article 243 (money laundering) of the CC.

Operational needs supported by analysis and dissemination

326. The AML/CFT Department, that is part of the DCEC headquarters and has 23 staff members, is responsible for preparing analytical materials disseminated spontaneously and at the request of the LEAs and also collects and analyzes STRs filed by financial institutions and DNFBPs. Due to the high degree of automation of information processing and the application of a risk-oriented approach to STR analysis, this number of analysts is sufficient for operational and strategic analysis.

327. The financial investigation procedure is governed by the DCEC internal regulations, primarily by the Regulation on Analysis of AML/CFT/CPF Information. It takes the DCEC analytical units not more than 30 days to prepare responses to the incoming requests, but, in certain circumstances, this work is done more promptly.

328. The incoming STRs and other information (mass media, supervisory information) are analyzed and responses to the incoming requests (including international requests) are prepared with the application of the RBA and depend on priority levels assigned to STRs or requests. The special colour-coding system (like traffic lights) is used, where the red or yellow markings correspond to high or very high risks identified in the NRA or indicate ML/TF or predicate offences, and such information is processed as a matter of priority. The "red" information is processed within a maximum of 5 days, while the "yellow" information is processed within not more than 10 days.

Case Study 6.5

On 11.11.2020, the DCEC received the STR regarding the I.M.B. company that was suspected of being involved in illegal cashing out activities by way of carrying out fictitious sale transactions.

The DCEC conducted an expedited financial analysis that revealed the following:

- There were discrepancies in the range of allegedly traded goods, for which payments were made and received;
- The company that lacked necessary material, technical and labour resources received large amounts of funds for the allegedly provided construction and assembly services;
- The director of the company was obviously the nominee, as he was earlier repeatedly convicted for economic crimes under the CC.

On 12.11.2020, based on the findings of the conducted financial analysis, the DCEC issued the order to suspend transactions of I.M.B. company for 30 business days.

On 19.11.2020, the DCEC received another STR regarding P.K.B. company.

Upon receipt of this STR, the DCEC conducted a financial analysis of financial transactions carried out by P.K.B. company and established that the counterparties of I.M.B. company started to transfer funds to P.K.B. company, which was also involved in fictitious sale transactions similar to those carried out by I.M.B. company.

On 20.11.2020, based on the prepared analytical report, the order was issued to the bank instructing it to suspend transactions of P.K.B. company for 30 business days.

The analytical reports concerning I.M.B. and P.K.B. companies were disseminated to the DCEC local office for conducting OIMs.

The OIMs findings revealed that individuals A, B and SH, acting for personal gain, established the organized criminal group and operated shell companies I.M.B. and P.K.B., which illegal activities inflicted exceptionally large losses amounting to UZS 3.1 billion on the State.

Besides that, the executive officers of bank X neglected their official duties and failed to take measures provided for in paragraphs 22, 54 and 62 of the ICR (No.2886 dated 23.05.2017). Therefore, they knowingly allowed the aforementioned companies to conduct shady economic activities (including cashing out transactions) and inflict exceptionally large losses on the State.

The criminal proceedings were initiated against the executive officers and shadow directors of the aforementioned companies under Article 184, Part 3 (evasion of axes or other mandatory payments)

and Article 189, Part 1 (violation of trade and services provision regulations) and also against the executive officers of bank X under Article 207, Part 1 (neglect of official duties) of the CC.

329. The LEAs note that, typically, they receive responses to their requests within less than 30 days (within 15 days on average). But even low-priority requests, responses to which are prepared with the use of the DCEC's own resources only, are processed within not more than 10 days. If a longer time period is required for obtaining the requested information (e.g. when requests are sent abroad), the DCEC, first, disseminates the interim information and after that, upon receipt of the necessary information, further provides it to a requesting party. This ensures prompt information exchange between the FIU and LEAs.

330. The preparation of analytical materials by the DCEC involves the collection and analysis of information from different sources. When a deeper financial analysis is required, this includes the following:

- Collecting preliminary information, inter alia, from the DCEC database and from entities that have sent STRs, and developing the plan of further actions;
- Collecting information and analyzing the collected data;
- Identifying schemes of ML, TF, PF and predicate offences (if the relevant indicators are available);
- Sending requests (if necessary), *inter alia*, to foreign competent authorities;
- Assessing the results of financial analysis and making decisions based on these results.

331. The analytical materials generated by the DCEC frequently include additional information, *inter alia*, financial information received from the competent authorities and the collected criminal intelligence. The DCEC analysis and disseminations are used by the LEAs for arranging and conducting OIM as well as for making further procedural decisions. A considerable part of materials received by FIU are used to initiate criminal cases by LEA; notably, the most results are demonstrated when the materials are used by operational units of the Department.

Table 6.11: Efficiency of Use by LEAs of (ML and Predicate Offences Related) Analytical

LEAs	2016		2017		2018		2019		2020	
	Spontaneous	At request	Spontaneous	At request	Spontaneous	At request	Spontaneous	At request	Spontaneous	At request
GPO		146 (33%)		31 (11%)		37 (13%)		20 (8,5%)		55 (52%)
SSS		25 (100%)		5 (100%)				3 (42%)	4 (100%)	15 (44%)
MIA		13 (87%)		4 (29%)		3 (75%)	-	18 (85%)	3 (100%)	17 (63%)
SCC							1 (100%)	1 (25%)	-	3 (100%)
DCEC Units	52 (72%)	343 (100%)	85 (69%)	358 (99%)	84 (52%)	414 (98%)	150 (30%)	426 (99%)	553 (37%)	169 (89%)

332. It should be noted that the number of criminal proceedings initiated by the DCEC operational units with the use of analytical materials disseminated by the FIU grows every year, which supports the assessors' conclusion about the high quality of these materials and the effectiveness of proactive efforts of the FIU, since this growth is driven, among other things, by the significant increase in the number of spontaneous disseminations in 2019-2020.

Table 6.12. Statistics on Criminal Proceedings Initiated by DCEC Operational Units

Time Period	Total Number of Initiated Criminal Proceedings	Including:	
		Based on AML/CFT Disseminations	Percentage of Total Number of Initiated Criminal Proceedings
2016	5,369	395	7.4 %
2017	4,753	443	9.3 %
2018	4,181	498	11.9 %
2019	3,517	576	16.4 %

2020	3,530	722	20.4%

333. Predicate offences most frequently initiated by operational units of DCEC based on the FIU analysis and disseminations are related to corruption (1021 criminal cases), tax offences (904 criminal cases), violation of trade and service provision regulations (230 criminal cases), foreign exchange offences (222 criminal cases) and fraud (58 criminal cases), which is consistent with the risks identified upon the results of the 2019 NRA.

334. As mentioned in section 6.1 above, over 60% of ML-related criminal proceedings are initiated by the DCEC operational units with the use of information provided by the FIU.

Table 6.13: Statistics on ML-Related Criminal Proceedings Initiated by DCEC Operational Units

Time period	Total number of initiated criminal proceedings	including:	
		Based on FIU Disemination	Independently
2016	58	32	26
2017	43	29	14
2018	48	34	14
2019	25	20	5
2020	27	13	14

335. The Uzbek authorities have also demonstrated to the assessors that other LEAs regularly initiate criminal proceedings using the disseminations received from the DCEC. As shown in the table below, the LEAs initiated 395 criminal proceedings based on the DCEC disseminations in 2016-2020. As mentioned above, most criminal proceedings were launched for predicate offences, but some of them were initiated for ML as well.

Table 6.14: Statistics on ML-Related Criminal Proceedings Initiated by LEAs Based on DCEC Disseminations (ML/ predicate offences)

#	Categories of Criminal Offences (ML/ predicate offences)	2016-2020			
		GPO	SSS	MIA	SCC
1	Money laundering	58	5	5	0
2	Human trafficking and migrant smuggling	0	0	5	0
3	Corruption	123	27	5	0
4	Illegal acquisition and sale of foreign currency	0	0	3	0
5	Fraud	9	0	31	0
6	Tax offences, illegal business activities, fake bankruptcy	68	12	0	2
7	Violation of trade regulations	25	0	0	0
9	Forgery	4	0	0	0
10	Other	0	0	0	0
11	Illegal trafficking in narcotic drugs and psychotropic substances	0	0	2	0
12	Illegal raising of funds and (other) other assets	0	2	2	0
13	Extortion	0	0	2	0
14	Theft	0	0	1	0
15	Smuggling	2	2	0	0
	Total	289	48	56	2

336. Similar to the DCEC operational units, other LEAs also request information from the FIU, primarily for investigating criminal offences that are most harmful for the economy and financial system, such as corruption, tax offences, violations of trade regulations and money laundering.

Case Study 6.6 (Cooperation of DCEC with the national LEA at request)
The DCEC conducted a parallel financial investigation at the request of the Investigation Department of the MIA in the course of the fraud-related criminal proceedings initiated against executive officers of the NVA company.

Individual X founded the NVA company and established the criminal group. After that, from 30.11.2018 through 13.09.2019, the executive officers of this company provided employment services to the citizens of the Republic of Uzbekistan promising to them jobs in different European countries. With the aim of taking possession of other persons' property by way of deceit or abuse of trust, the executive officers fraudulently signed contracts with individuals and collected one-time fee in the amount of USD 1,000 up to 3,500, however, none of those individuals actually obtained employment and travelled abroad. Nearly one thousand individuals suffered from the fraudulent activities of the company, and total losses incurred by them exceeded USD 3 million.

Upon receipt of the request, the DCEC searched for information about the suspects in all databases with the use of all available and accessible information resources and eventually established the following:

- The main portion of the collected funds was transferred by the company to the money laundering service providers (firms that provided money laundering services) for the purchase of various unrelated goods and services;
- Analysis of current accounts showed absence of transactions involving the transfer of funds abroad;
- The company did not indicate goods and services purchased by it from the money laundering service providers in the submitted tax statements;
- After the registration of the company, its executive officers purchased real estate property in Tashkent city and the Tashkent region as well as Captiva and Lacetti cars which were registered in the names of their close relatives.

The collected information and documents were submitted to the Investigation Department of the MIA which initiated criminal proceedings, *inter alia*, under Article 246 (legalization of proceeds obtained through crime (money laundering)) of the CC.

The court found the executive officers of the company and other defendants guilty and sentenced them to imprisonment and ordered to confiscate property acquired by them with the proceeds of the said criminal offence.

337. A certain decline in the number of initiated criminal proceedings related to ML and predicate offences and a decrease in the number of requests filed by the LEAs (primarily the prosecution authorities) can be explained by the provisions of Decree No.UP-4725 of the President of the Republic of Uzbekistan "On measures to ensure reliable protection of private property, small businesses and private enterprises and to remove barriers for facilitating their accelerated development" which came into force on May 15, 2015. This Decree provides that criminal proceedings should not be initiated and a person should be released from liability for the offence criminalized under Article 184 (evasion of taxes and other mandatory payments) of the Uzbek Criminal Code committed for the first time if such person fully compensated losses inflicted on the State and paid penalty and other types of financial sanctions within 30 days following the detection of such criminal offence.

338. Upon identification of indicators of possible tax crimes, the DCEC proactively sends notices for preventing these crimes and collecting unpaid taxes, which helps to promptly compensate inflicted losses.

Table 6.15: Statistics on Notices Disseminated Based on the FIU Materials

	2016	2017	2018	2019	2020	Total
Number of notices disseminated by DCEC based on FIU materials	7	21	51	286	590	955
Taxes paid upon receipt of DCEC notices, USD mln	0.5	0.7	0.9	3.5	9.7	15.3
Materials filed for use in criminal proceedings	3	5	10	14	23	55

339. Similar to ML-related disseminations, the FT-related analytical materials disseminated by the FIU are also highly demanded by the law enforcement agencies, as evidenced by a stable ongoing exchange of information both at the request and spontaneously. The statistics on FT-related criminal

proceedings initiated by the LEAs (Interior Ministry and State Security Service) based on the FIU disseminations support this conclusion.

Table 6.16: Statistics on TF-Related Criminal Proceedings Initiated by LEAs Based on DCEC Disseminations

TF Investigation Agency	2016	2017	2018	2019	2020	Total
SSS		1	1	2	1	5
MIA			2	2	5	9
Total		1	3	4	6	14

340. In 2016-2020, fourteen (14) TF-related criminal proceedings were launched based on the DCEC disseminations, which accounted for 31% of the total number of criminal proceedings initiated in the country. The increase in the number of criminal proceedings initiated based on the FIU disseminations also correlates with the growing volume of analytical materials provided by the FIU spontaneously and at request (Table 6.4). This demonstrates the extensive use of analytical materials generated by the FIU for CFT.

341. The DCEC conducts ongoing strategic analysis which results are used for pursuing tactical objectives as well as for achieving the strategic goals with a view to mitigating ML/TF risks in the country. Based on the strategic analysis outcomes, the relevant guidelines are provided to the private sector entities through their respective supervisors, and changes and modifications are introduced into the legislation and the ICRs of reporting entities.

342. The reasons for conducting strategic analysis include the surge in information flows from FIs as well as the results of studying the international experience and reviewing the operational situation in the country.

343. The results of the conducted d analysis align with the risks identified in the country and are aimed at reducing the level of threats posed by such offences as fraud, violations of trade regulations and tax offences.

344. The analytical materials generated by the DCEC are provided to FIs and DNFBPs as the guidelines for identifying ML/TF risks and contributing to improving the quality of STRs. In the assessed period, the DCEC developed 23 typologies of ML and associated predicate offences, which were disseminated to the different government authorities, such as the Finance Ministry, SCC and STC for taking response measures within their purview as well as to the DCEC operational units for the criminal intelligence gathering purposes and to the CB for communicating them to credit institutions.

Case Study 6.7 (Examples of strategic analysis)

1) Analysis of STRs related to international money transfers by natural persons, where multiple individuals send money to the same recipient. The analysis was conducted every 6 months from 2016 through 2017.

Reason for conducting analysis: Large number of incoming STRs.

Outcomes: The analysis findings were disseminated to the DCEC OIA units for criminal intelligence gathering purposes and resulted in the initiation of over 40 criminal proceedings.

2) Analysis of suspicious transactions related to termination by natural persons of the cellular communication service agreements after accumulation of a certain amount of funds on their current accounts. The analysis was conducted in the second half of 2019 in cooperation with the cellular communication service operators.

Reason for conducting analysis: Review of international practices – typologies of ML and associated predicate offences.

Outcomes: Info letters were circulated recommending the obliged entities to report such transactions to the DCEC if the transaction amount exceeds 100 base calculation values.

3) Analysis of services provided by the payment system operators for identifying vulnerabilities in the offered services that contribute to the materialization of potential ML/TF/PF threats. The analysis was conducted at the beginning of 2019 in cooperation with the payment system operators.

Outcomes: Adoption of internal control rules for payment service providers payment processors, payment

system operators and e-money system operators (Reg. No.3266 dated 30.06.2020); and adoption of the Law on Payments and Payment Systems dated 19.09.2019.

Table 6.17: Examples of Typologies

Typology: Cashing out funds and laundering criminal proceed by carrying out multiple P2P transfers between natural persons	– DCEC operational units (for gathering criminal intelligence); – STC (for taking preventive measures); – Central Bank (for informing commercial banks).
Typology: Embezzlement of the state budget funds by holding tenders with participation of affiliated companies and entering into public procurement contracts with predetermined business entities	– DCEC operational units (for gathering criminal intelligence); – Anti-Corruption Agency (for taking preventive measures); – Audit Department of Finance Ministry (for taking preventive measures); – Central Bank (for informing commercial banks)
Typology: Embezzlement of the state budget funds by entering into multiple public procurement contracts for the supply of the same type of goods/ products for bypassing the official tender process	– DCEC operational units (for gathering criminal intelligence); – Anti-Corruption Agency (for taking preventive measures); – Audit Department of Finance Ministry (for taking preventive measures)

345. In general, the ongoing strategic analysis not only has a positive impact on the identification of criminal offences and initiation of criminal proceedings for predicate offences but also improves the effectiveness of the entire AML/CFT/CPF system of Uzbekistan.

346. In practice, the DCEC also cooperates with the CB in case of detection of potential breaches of the specific or AML/CFT legislation in the course of conducting OIM by DCEC.

Table 6.18: Statistics on Joint Actions Taken in Cooperation with the Central Bank

Time period	Number of joint actions	Total number of initiated criminal proceedings
2016	2	2
2017	3	3
2018	4	4
2019	14	13
2020	11	10
Total	34	32

Case Study 6.8 (Cooperation with the oversight authorities based on OIM gathered by DCEC)

The DCEC summarized and analyzed the case files related to criminal proceedings initiated against the executive officers of several shell companies based on the OIM findings. Following the review of these criminal case files, it was established that 6 shell companies had accounts opened with the branch of the Bank and were involved in illegal cashing out activities by way of carrying out large transit transactions in 2016-2017.

Despite the fact that those companies carried out unusually large transactions that had no apparent economic or lawful purpose, the Bank had neither conducted enhanced CDD nor filed STRs with the FIU.

The detailed and summarized reports were provided to the regulatory authority – the CB, which confirmed the facts of several violations of the AML/CFT/CPF legislation in the course of a supervisory inspection.

Following the inspection, the CB applied financial sanctions against Bank in amount of UZS 1 billion, which exceeded by ten times the revenues received by the bank as fees paid by the shell companies.

Besides that, strict disciplinary sanctions (including dismissal from the office) were applied against several executive officers of the bank.

347. In general, the high effectiveness of analytical materials generated by the DCEC and regular use of such materials for initiating criminal proceedings shows that analysis conducted by the FIU supports, to a large extent, the operational needs of both FIU operational units and other LEAs when they request such support. Spontaneous disseminations by the FIU are also highly demanded and regularly used for initiating criminal proceedings.

348. One of the strengths of the Uzbek FIU is that it closely monitors the further application of analytical materials disseminated spontaneously to its own operational units, which increases the efficiency of their practical use. The practice of joint OIM also plays a significant role in communicating financial intelligence to the competent authorities, since a large number of criminal proceedings are initiated based on the OIM findings.

Cooperation and exchange of information/ financial intelligence

349. Uzbekistan has arranged for sound interagency cooperation. As noted in IO.1, the interviewed LEA officers mentioned close AML/CFT cooperation and coordination at both high and operational levels.

350. The DCEC is the core to the functioning of the Uzbek AML/CFT/CPF system. The DCEC has signed cooperation and information sharing agreements with over 30 ministries and government agencies, and the FIU has access, including direct access, to a wide range of databases. Analytical materials are exchanged on an ongoing basis via secure communication channels (examples were demonstrated to the assessment team), which enables to maintain a high enough level of understanding of the current risks and typologies consistent with the NRA findings.

351. In 2016-2020, the prosecution authorities established 957 investigation teams for investigating complex multiple crime cases involving corruption, economic and organized crime. These teams are composed of prosecutors (about 50% of personnel) and officers of the FIU (25%), the MIA (20%) and the SSS (5%), which has allowed the country to improve the effectiveness of investigations into the aforementioned categories of criminal offences.

352. The DCEC conducted, in cooperation with the SSS, the MIA and the SCC, over 4,300 joint OIMs that resulted in the initiation of more than 4,100 criminal proceedings, including 5 criminal proceedings for ML.

353. The DCEC conducts strategic analysis and identifies typologies of ML/TF and other criminal offences that are regularly communicated to all competent authorities and, where appropriate, to the private sector.

354. Joint training events and roundtables are regularly arranged for all AML/CFT system stakeholders. In particular, 37 training courses were delivered in 2016-2020 for the officers of the DCEC operational units, which allowed 963 operatives, inquirers and auditors to receive professional development training. Each year, several training events are also arranged, in cooperation with the Academy of the GPO, for officers of other LEAs. Besides that, knowledge and experience are shared in the process of operation of joint investigation teams and in the course of joint operational meetings.

355. The DCEC initiates a large number of training events, in form of workshops, webinars, training courses and roundtables, for the supervisors and private sector, with 20 such events held in 2020, nine events held in 2019, eight events held in 2018 and seven events held in 2017.

356. There are no legislative restrictions that may hinder cooperation and exchange of information and financial intelligence among the FIU and other competent authorities, except for information constituting state secrets. For the purpose of discharging the assigned functions, the competent authorities are empowered to request and receive the required information, including confidential information subject to the application of non-disclosure safeguards. The DCEC is authorized to disclose bank secrecies in its disseminations to the LEAs.

357. There are feedback mechanisms in place to monitor the effectiveness of use by the LEAs of information disseminated to them both at the request and spontaneously. Feedback as per the established form is provided in response to each dissemination. There is also the practice of appointing particular officers personally responsible for the use of received disseminations. At the

same time, the LEAs designate the contact officers for more prompt information sharing and cooperation.

358. The DCEC and its officers ensure confidentiality and security of information constituting commercial, bank and other secrets has become known to them. The DCEC officers are required to sign a non-disclosure agreement and in case of unauthorized disclosure of information, the officers are held liable under the applicable legislation. Access to the DCEC devices and information is also strictly governed by internal regulations.

359. Information (STRs, SARs, registration data, beneficial ownership information, information about directors and business activities, banking information, criminal intelligence, FIU analysis findings, etc.) received via the international cooperation channels from abroad is disseminated to the relevant LEAs within the scope of their purview only upon authorization of the requested foreign FIUs and strictly for the purposes indicated by them.

360. The DCEC has built its own autonomous local information network that is not connected to the Internet and is divided into segments with different levels of access. The information security measures are set out in the relevant internal regulations. Special personal logins and passwords are assigned for accessing the DCEC information system. The use of external ports and removable media is governed by the relevant internal instructions and regulations. The DCEC building and territory are guarded by the Uzbek National Guard troops.

361. The databases of other government authorities and institutions are remotely accessed via the dedicated secure communication channels with the use of personal logins and passwords, including electronic digital signatures, provided by the relevant government authorities and institutions. Access to such databases is provided only for discharging the official functions. All government authorities have the mechanisms in place for ongoing monitoring of potential unauthorized access to the data held by them.

362. The DCEC shares information with the law enforcement, investigation, judicial and other competent authorities s through the postal (government courier) communication channels, and also via secure electronic communication channels. The disseminated financial information is intended for restricted circulation (for official or more limited use only). Classified information is shared in accordance with the legislation on the protection of state secrets.

363. The AML/CFT/CPF system of the Republic of Uzbekistan is featured by the high level of cooperation for both sharing financial intelligence and communicating the results of strategic analysis and new typologies and schemes of ML and predicate offences. Close cooperation is arranged with the supervisory authorities. All information and data are reliably protected by way of application of a wide range of information and physical security measures.

Overall conclusions on IO.6

364. The LEAs have access to a wide range of financial information and intelligence both directly and through the use of the FIU resources. The DCEC is the core of the functioning of the national AML/CFT/CPF system of Uzbekistan and actively disseminates information to other LEAs both spontaneously and at request as well as in the course of joint OIMs. Financial information obtained based on STRs and through access to various databases is used to a full extent for identifying and investigating TF and predicate offences. However, ML cases are identified primarily by the DCEC, while other LEAs pay less attention to this problem. Besides that, there is no evidence of active use of available financial information for tracing criminal proceeds.

365. The intelligence generated by the FIU based on incoming STRs and other reports (including currency cross-border transfer reports) is actively used for conducting financial investigations. Besides that, prompt decisions can be made based on STRs to freeze funds for ensuring their security and disrupting criminal offences. A certain drawback is a fact that the FIU has only information provided by financial institutions (primarily by banks), which may limit the ability to proactively identify ML and predicate offences.

366. Analysis conducted by the FIU supports, to a large extent, the operational needs of both DCEC operational units and other LEAs. A large portion of DCEC disseminations is used for initiating criminal proceedings by all LEAs.

367. **The Republic of Uzbekistan is rated as haing a substantial level of effectiveness for IO.6.**

Immediate Outcome 7 (ML Investigation and Prosecution)

ML identification and investigation

368. The pre-trial activities involving the detection, suppression, solving, and investigation of ML crimes in the Republic of Uzbekistan take the form of OIA and pre-trial proceedings in criminal cases and files. Pre-trial proceedings consist of two stages: a pre-investigation check and a preliminary investigation (inquiry or preliminary investigation). Depending on the complexity of a crime, its detection, solving, and investigation can combine various forms (e.g., OIA, a pre-investigation check, and a preliminary investigation) or be conducted only as a preliminary investigation that is necessary for ML cases.

ML crime identification and prevention

369. ML crimes can be identified and supressed during OIA by any authority that performs OIA (bodies of the MIA, the SSS, the Presidential State Security Service, the military intelligence of the MO, the SCC, the DCEC, and the Bureau of Compulsory Enforcement under the GPO (BCE)).

370. ML crimes can also be identified during a pre-investigation check and a preliminary investigation.

371. Given the information provided by the country, a vast majority of ML facts were identified either directly by a preliminary investigation authority when investigating criminal cases on predicate crimes or during OIA as part of criminal intelligence assistance (support) in the investigation of predicate crimes. This practice stems from the impossibility to prosecute one for ML without charges or conviction for a predicate crime and may also indicate that the LEAs are focused on identifying predicate crimes on a priority basis which cannot help but ultimately affect the identification of conspiratorial groups of professional launderers, money laundering by third parties, or when a predicate crime is committed outside the country.

372. This is confirmed by available statistics on identified ML crimes.[35]

Table 7.1. General data about the number of ML investigations (identified crimes) by all prosecution authorities

Form of money laundering:	2016	2017	2018	2019	2020	Total
- ML by third parties	2	1	2	1	1	7
- ML when there is no conviction for a predicate crime						
- self-laundering	88	87	71	37	47	330
- ML when a predicate crime is committed in another country				1		1
Total ML investigations:	90	88	73	39	48	338

373. Available information suggests that the identified facts of ML were self-laundering in the majority of cases (97.6%). Third parties identified ML in individual cases (seven cases).

374. In view of this, the above data indicate that the detection of ML crimes committed by third parties is insignificant. At the same time, persons (groups of persons) specialised in the “professional” laundering of criminal property pose the greatest danger in the criminal area of ML. Such groups usually do not commit ML predicate crimes but derive their criminal proceeds as payment for services relating to valuables laundering. Given the low efficient identification of ML committed by third

[35] Here and elsewhere, it should be considered that statistics repeatedly provided by the competent authorities differed in terms of the same items and depending on the authority that provided it. The assessors attempted to rectify differences in statistics during the onsite visit but it was not possible to rectify all the deficiencies. Representatives of the competent authorities ascribed such discrepancies to differences in the methods of recording and transferring statistics from one body to another (from the GPO to the MIA) and to the fact that data changed over time.

parties and the absence of any case studies where the activities of professional launderers were identified, the assessors conclude that the LEAs do not pay adequate attention to this area of AML.

Case Study 7.1.
Mr N, after committing theft by appropriating property and other crimes, derived criminal proceeds in especially large amounts. To launder these, Mr N moved out the funds (USD 5 million) abroad via a firm he owned, and another person (a professional launderer) purchased there 98 gold bars weighing 68 kg and costing USD 4.4 million and kept them in a foreign bank. During the preliminary investigation, Mr N voluntarily handed over all the gold bars as payment of the criminal proceeds, and this property was confiscated and forfeited in favour of the state based on a court judgment.

375. Data presented in Table 7.1 suggest that the country shows a characteristic downward trend in terms of the number of ML-related identifications and instituted criminal cases. Compared with 2016 figures, the number of instituted cases decreased by 45.2% in 2019 and by 35% in 2020.

376. This pattern can be accounted for, to a certain extent, by a decrease in the overall number of predicate crimes which based on available data decreased by 44.7% in 2019 (compared with 2016) and by 42.9% in 2020.

377. Legislative liberalisation also played a certain role in this, in particular, that it is possible not to institute a criminal case for tax evasion and not to launch an investigation provided that compensation for damages is paid in full.

378. Additionally, LEA representatives ascribed this pattern to the fact that, in doing their work, they started paying greater attention to the identification of graver ML crimes that entailed a large-scale ML. As the country has no threshold approach for ML prosecution purposes, the assessors believe that, in order to ensure the unavoidability of liability of the guilty persons, the LEAs should focus their efforts on identifying all facts of ML irrespective of the amount of laundered criminal proceeds.

379. The share of identified ML crimes in relation to the overall number of committed predicate crimes is small. That this share of ML investigations is small in relation to predicate crimes objectively stems – in the majority of cases – from the fact that the derived criminal proceeds or property was used without changing its legal nature and without any actions aimed at concealing the true origin of such funds and property. Representatives of the competent authorities note that in most cases criminals do not need to take action to launder money since the amounts of criminal property or funds they derived are small, and their criminal origin is not obvious, in view of which simply using their criminal proceeds does not arouse any suspicions about its criminal origin.

380. However, the assessors also believe that, apart from the above objective reason, there are a number of subjective ones. These include both focus on solving predicate crimes on a priority basis, inadequate attention to the importance of OIA aimed at exposing conspiratorial ML schemes and persons involved in them, and that the prosecution authorities do not have a uniform understanding and a common practice when conducting financial (parallel) investigations.

381. The current situation surrounding the division of ML identification and prevention powers also affects this.

382. In terms of identifying ML crimes, the main pressure is on the DCEC which is the FIU and authority responsible for the state of this work. Statistical data suggest that, in 2016–2020, the DCEC conducted 657 pre-investigation checks of materials having indications of ML,[36] with 201 criminal cases opened under Article 243 of the CC[37], which is 59.6% of the overall number of ML cases opened by all authorities. Besides, in 73 cases, indications of ML were identified during OIA, and in 128 cases – during financial (parallel) investigations during the investigation of criminal cases on predicate crimes.

[36] The assessors treated the institution of an ML criminal case as the identification (detection) of such a crime. To assess the activities of investigative divisions, the assessors used the criterion of the number of cases referred to court.
[37] In other cases, materials of pre-investigation checks resulted in the institution of criminal cases on predicate crimes.

383. Additionally, activities of the DCEC are not limited only to the identification of crimes that fall within the remit (investigative jurisdiction) of the prosecution bodies conducting a preliminary investigation in most crimes that fall within the subject-matter jurisdiction of the DCEC as a body engaged in OIA.

Case Study 7.2

When performing OIA, the DCEC established that Mr G, between 2016 and 2018, created an international telephone IP communication system and provided illegal services that consisted of citizens of Uzbekistan and Russia maintaining telephone communication with each other, and derived criminal proceeds amounting to USD 61.3 thousand.

Mr G laundered the above money by purchasing cars fictitiously registered under the ownership of third parties in order to lend a veneer of legality to the origin of the criminal proceeds.

The DCED opened a criminal case under Articles 278-1 (Breach of informatisation rules) and 243 (ML) of the Criminal Code that was transferred to the MIA in accordance with its investigative jurisdiction.

In a judgment, Mr G was found guilty and convicted for the above actions to imprisonment, while the purchased cars were forfeited in favour of the state.

384. The MIA, despite the fact that ML cases fall directly within its investigative jurisdiction, yielded far modest results. The internal affairs authorities identified ML crimes (with the exception of one criminal case) only when it came to predicate crimes assigned to their investigative jurisdiction and as part of the investigations of the same that were already ongoing.

Table 7.2. Data on the number of ML criminal cases opened by the internal affairs authorities broken down by predicate crime

Predicate crime:	2016	2017	2018	2019	2020	Total
- Theft	1	3	1	3	1	9
- Fraud	2	5	2	4	17	30
- Embezzlement by spending	1	1			1	2
- Brigandage		1				1
- Robbery			1			1
- Extortion				1		1
- Unlicensed activity					1	1
- Forgery of documents			1		1	1
Total	4	10	5	8	20	47
ML criminal cases without any simultaneous investigation of predicate crimes	1					1

385. As for the identification of ML crimes by divisions of the State Security Service, they took such efforts to the extent of their statutory powers to identify and investigate predicate crimes that fall within their remit.

Table 7.3. Data on the number of ML criminal cases opened by the bodies of the State Security Service broken down by predicate crime

Predicate crime:	2016	2017	2018	2019	2020	Total
- Embezzlement by appropriation or spending	2	1		1		4
- Fraud		2	1			3
- Breach of customs law			3	1	1	5
- Tax evasion or evasion of other obligatory payments	4		1			5
- Illegal production, acquisition, storage, and other actions involving drugs, their analogues, or psychotropic substances for the purpose of selling them, and sale of the same		1				1
- breach of rules of trade or service	1					1
- Passive bribery	1					1
All ML cases:	8	4	5	2	1	20

386. The assessors think that assigning the ML crime to the exclusive investigative jurisdiction of the MIA may lead to the bodies performing OIA becoming disinterested in identifying such crimes on their own since, in essence, the identification of the ML crime is not one of their principal duties.

387. It should be also noted that all work related to the identification of ML crimes is performed by the DCEC, the MIA, and the SSS. Other bodies performing OIA either did not identify ML by virtue of the specific nature of their activities (the Presidential State Security Service, the military intelligence of the Ministry of Defence, the BCE) or this identification was aimed at cooperating with the DCEC, the MIA, and the SSS generally as far as predicate crimes were concerned (SCC).

388. To identify ML, the LEAs use all available OIM during OIA, including by conducting them in a comprehensive manner. There are cases when predicate crimes and ML are identified following the verification of information distributed in the mass media or on the Internet.

Case Study 7.3
The article "Jizzakh-Style Tender" was distributed online and concerned the allocation of construction facilities to people closest to Mr R, Deputy Hokim of the Jizzakh Region (Deputy Head of the local administration).
An inspection revealed that Mr R transferred construction facilities to his relatives without any tenders, with approximately USD 8.5 million being later embezzled by overstating the amount of work performed.
The DCEC established that the criminal proceeds and property assessed at USD 9.1 million were laundered.
Criminal cases were opened in respect of Mr R and 12 accomplices under Articles 167 (Embezzlement by appropriation or spending on an especially large scale), 205 (Abuse of power or official duties causing considerable damage), 209 (Forgery in public office), 243 (ML) of the CC.
https://www.gazeta.uz/ru/2021/01/22/jizzax/
https://t.me/senatuz/7474

389. Bodies engaged in OIA have a good level of cooperation that consists of joint OIM, priority inspections, and the exchange of criminal intelligence. They engage in such cooperation mostly with the DCEC when identifying and preventing predicate crimes, though there are cases when they take joint action, including criminal intelligence ones, aimed at identifying ML proper. In 2016–2018, the DCEC is found to have cooperated with the bodies of the SSS (five cases).

390. In 2019–2020, bodies engaged in OIA did not take joint action to identify and prevent ML proper, though there were cases when joint OIM resulted in the identification of predicate crimes and then ML.

Case Study 7.4
Mr I, conspiring with four accomplices for fraud purposes, created a limited liability company.
Between 2018 and 2019, under the guise of selling seedlings of valuable species, they collected a significant amount of money from people.
To launder their criminal proceeds, they later purchased in the name of various persons real estate units totalling UZS 3 billion and cars totalling UZS 710 million.
These facts were identified in the course of joint OIM and pre-investigation measures performed by the MIA and the DCEC, following which the Investigative Department of the MIA opened a criminal case under Articles 168 (Fraud) and 243 (ML) of the CC.

Pre-trial proceedings (preliminary investigation) involving ML cases

391. The pre-trial investigation of ML criminal cases is carried out by investigators of the internal affairs authorities (MIA) in accordance with the general rule set forth in Article 345 of the CPC. However if an ML crime is identified during the preliminary investigation of a predicate crime, the ML investigation can be carried out by an investigation body authorised to investigate the predicate crime (the prosecutor's office, the MIA, and the SSS) as part of one criminal case involving the predicate crime.

392. In addition, the main objective of the investigator carrying out the preliminary investigation of the criminal case is to collect, record, and procedurally formalise evidence in the criminal case, to assess the totality of the evidence in terms of its sufficiency for bringing charges and referring the case to court, to bring charges against persons whose involvement in the crime is proven.

393. With that said, the investigator does not have such functions – which representatives of the body engaged in OIA have – as the identification and suppression of ML crimes. However, the investigator can identify the fact that a person committed an ML crime during the ongoing investigation of a predicate crime based on the assessment of the evidence available in the case and the established facts.

394. Statistics of investigated ML crimes that resulted in the relevant criminal cases being referred to court do not materially differ from the number of opened ML cases, which indicates that proceedings related to such facts are terminated in isolated cases and this does not considerably affect the effectiveness of ML identification and investigation.

Table 7.4. General data on the number of completed (referred to court) ML criminal cases by all prosecution authorities

Form of money laundering	2016	2017	2018	2019	2020	Total
- ML by third parties	1	1	2	1	1	6
- ML when there is no conviction for a predicate crime						
- self-laundering	86	87	71	37	47	328
- ML when a predicate crime is committed in another country				1		1
Total ML investigations:	87	88	73	39	48	335

395. Investigative divisions of the Interior Ministry, which have direct investigative jurisdiction over the preliminary investigation of ML cases, investigated only 13.9% of the total number of cases under Article 243 of the CC. This figure is accounted for by the existing practice of determining investigative jurisdiction for a predicate crime that is already investigated.

Table 7.5. The pattern of criminal cases on ML crimes referred to court

Law enforcement authority	2016	2017	2018	2019	2020	Total
Prosecutor's Office	75	74	63	29	27	268
Interior Ministry	4	10	5	8	20	46
State Security Service	8	4	5	2	1	20
Total	86	88	73	39	48	335

396. As concerns specialisation, ML criminal cases are investigated by the prosecution bodies based on categories of predicate crimes. The GPO has departments (and their regional divisions) for combating organised crime and corruption, for investigating especially grave crimes. A structural division, to which competence in the investigation of a predicate crime falls, also investigates ML criminal cases. An agency-level regulation established that the investigation of especially complex multi-episode cases, including those involving predicate crimes and ML, is carried out by senior major case investigators of departments and their regional divisions.

397. If the investigation of an ML criminal case needs to be assigned high priority, the prosecution bodies apply generally elaborated approaches to ensuring the comprehensiveness, impartiality, and promptness of the investigation: (i) an investigation group is created (including an interagency one), (ii) criminal cases are elevated to higher divisions and the headquarters, (iii) criminal cases from different regions are consolidated into one proceeding in the headquarters, (iv) the prosecution bodies request other LEAs to provide materials of the pre-investigation check and criminal cases.

398. As concerns specialisation, ML criminal cases are also investigated by the internal affairs authorities based on categories of predicate crimes. For example, the Investigative Department of the MIA has structural divisions: a department for investigating corruption, economic crimes, and fraud; a department for investigating information technology crimes; a department for investigating crimes involving drug trafficking and organised crime; a department for investigating crimes against the person.

399. It is notable that the LEAs investigate ML cases involving organized criminal groups (OCGs).

Case Study 7.5
Senior officials of an industrial enterprise, acting as an organised group, released unaccounted products that they sold in secret for cash in violation of the applicable rules of trade and distributed proceeds

among the members, avoiding paying taxes on the same. They provided knowingly false information and data in the accounting and production records intending to conceal the traces of their crime by decreasing the output of finished products and overstating the consumption of raw materials.
Operational divisions of the MIA together with the DCEC conducted a controlled purchase operation and bought unaccounted-for products, following which a criminal case was instituted under Articles 167 (Embezzlement), 227 (Forgery of documents) of the CC.
During the investigation, in order to establish the actual scale of criminal activities of the OCG and laundered proceeds, technically complex and labour-intensive expert examinations and audits were commissioned and OIMs were performed, following which the organised group was found to have acted at the enterprise for three years, and over this period they concealed from accounting records and sold in secret finished products for more than UZS 38 billion, causing damage to the shareholders and avoiding paying taxes amounting to around UZS 4 billion.
Twenty two cases were also found when the members of the organised group gave bribes to nine employees of the controlling authorities totalling USD 40 thousand in order to facilitate and conceal their crimes.
The members of the organised group laundered criminal proceeds by purchasing various properties and opening business structures in their names and in the names of their relatives and other front persons.
After the investigation, 14 members of the organised group were held criminally liable under Articles 167 (Embezzlement), 184 (Tax evasion), 211 (Active bribery), 228 (Forgery of documents), and 243 (ML) of the CC. The nine officials who accepted bribes were held liable under Article 210 (Passive bribery) of the CC. Laundered proceeds amounting to UZS 35 billion were seized.

400. The SSS has a similar specialisation when it comes to the investigation of ML cases based on categories of predicate crimes.

401. At the preliminary investigation stage, the country widely practices creating interagency investigation groups that include representatives of various LEAs, including the FIU. In 2016–2020, the prosecution bodies created 957 investigation groups for investigating multi-episode and especially complex criminal cases, and 724 employees of the prosecution bodies, 366 employees of the DCEC, 304 employees of the MIA, and 64 employees of the State Security Service were involved in them.

402. Apart from being involved in interagency investigation groups, the FIU cooperates with investigative divisions of the LEAs by performing individual instructions of criminal investigators. The country has provided examples of such instructions, among other things, those related to the identification of bank accounts and other assets, the identification of BOs, verification of the actual owners of property for ML purposes, financial audits, and others.

403. Moreover, to find indications of ML and to identify and track criminal proceeds, funds intended for TF purposes, instruments of crime and other assets, including the property of equivalent value that may be forfeited in favour of the state, parallel financial investigations are carried out, and their procedure is established by joint orders of the GPO, the MIA, the SSS, and the SCC. In addition, such investigations are obligatory when it comes to ML/TF criminal cases and crimes that entailed significant damage or resulted in especially large proceeds.

404. It should be noted that a joint regulation governing the procedure for, the objectives and limits of, financial (parallel) investigations was adopted only in May 2021. At the meetings, representatives of the competent authorities demonstrated a different understanding of the objectives, methods, and sources of information during financial (parallel) investigations. In light of this, the assessors conclude that there had been no uniform methodology and practice of such investigations in the period preceding the adoption of the said regulation, which accordingly affected the quality of ML identification and ML investigation in general.

405. Specialists from other agencies are involved at the pre-trial stage of proceedings in the case, including in the course of parallel financial investigations. According to the GPO, 403 specialists from the STC, 306 specialists from the MF, 205 specialists from the DCEC (internal auditors), 148 specialists from the CB, and 492 specialists from other agencies were involved for the above purposes over the period in question.

406. However, the country also demonstrated to the assessors case studies of successful financial (parallel) investigations.

Case Study 7.6
A parallel financial investigation revealed that officials of "S" LLC, fraudulently and under the guise of selling ostrich chicks to individuals in order to repurchase them later at a larger price, took possession of funds of 319 citizens totalling UZS 3.8 billion. The funds were laundered by way of transfer from the settlement account of "S" LLC to a settlement account of a controlled legal entity under the guise of a financial loan and were then used for purchasing cars fictitiously registered under the ownership of third parties. It was established in the case that the guilty persons also committed other crimes. In its judgment, the court found the officials of the company guilty of fraud, tax evasion, breaches of the rules of trade, money laundering, and sentenced them to imprisonment.

407. Such form of cooperation as OIM and investigations carried out by interagency investigation groups helps successfully identify crimes, improve the promptness of prosecution and conduct of complex parallel financial investigations.

Case Study 7.7
When investigating a criminal case in relation to officials of clients and contractors of a strategic facility, the construction of which was funded from the government budget, the State Security Service created an interagency investigation group that included representatives of various LEAs, including the DCEC. In this criminal case officers of the DCEC examined the financial transactions of more than 60 business entities involved in the construction of the strategic facility. As a result, one identified illegal financial transactions (fictitious sale transactions) and mutual settlements for subcontracted works which were not actually performed, and that senior officials of the general contractors and subcontractors were affiliated with each other. The funds from the government budget transferred to the business entities (subcontractors) were found to have been subsequently transferred to the settlement accounts of the controlled legal entities, to payment cards of the founders and senior officials of these legal entities as gratuitous financial loans and dividends, cashed out and converted into foreign currencies. The parallel financial investigation also revealed movable and immovable property, including laundered ones. In its judgment, the court found the officials of the business entities guilty of crimes under Articles 167 (Embezzlement by appropriation), 205 (Abuse of power or official duties), 209 (Forgery in public office), 243 (ML) of the CC, with other elements of a crime involved as well. Some seized property was used as compensation for property damage amounting to UZS 3 billion, and some [seized property] amounting to UZS 2 billion was forfeited in favour of the state as criminal property.

408. See IO.8 for other case studies of successful parallel financial investigations, including interagency ones.

409. Apart from investigating ML criminal cases, the prosecution bodies in accordance with the law also supervise all OIA bodies, inquiry and preliminary investigation bodies to make sure their activities are law-based. When performing their supervision powers, prosecutors review criminal cases received from the prosecution bodies (in order to further refer them to court) in terms of the reasonableness of charges brought, including ML-related ones, or, on the contrary, the reasonableness of no charges brought. Besides, prosecutors examine whether the termination of ML proceedings was based on law or not.

410. Additionally, to promote the impartiality and quality of investigations, the prosecutor's office may provide written instructions on criminal cases that the investigator is obliged to follow. Heads of investigative divisions have similar powers when it comes to exercising agency-level control over investigators. The assessors were provided with case studies of written instructions on ML cases.

Case Study 7.8
When investigating a criminal case in relation to a director, Mr I, under paragraph "a" of Part 3 of Article 167, Part 3 of Article 184, paragraph "a" of Part 2 of Article 205, and Article 243 (ML) of the CC, the Head of the Department for the Investigation of Especially Grave Crimes of the GPO provided binding written instructions, including those related to the commissioning of an audit of financial and business

operations of “Ya” LLC, the recovery of documents concerning tax reports and collection transactions provided to a bank, the identification of property registered in the name of Mr I and his family members, the examination of proceeds of the accused person’s relatives with a view to establishing whether they could have purchased the property, the identification of funds, other assets, including the property of equivalent value that may be forfeited in favour of the state and confiscated.

411. Prosecutors are also entitled to revoke rulings of the prosecution bodies concerning the institution of a criminal case, the refusal to institute a criminal case, the suspension and termination of a criminal case. The GPO reports that, between 2017 and 2020, prosecutors revoked 235 rulings of the DCEC. However, prosecutors did not make any procedural decisions regarding the relevant rulings of the DCEC on ML cases and materials over the period in question.

412. The GPO reports that, in order to provide adequate support to the public prosecution, the FIU provides operational support also during the judicial examination of criminal cases if necessary.

413. Existing interagency agreements, joint instructions (e.g., joint instructions of the GPO, the SSS, the MIA, and the SCC concerning the procedure for examining financial aspects of criminal activity at the pre-trial stage, the procedure for identifying, storing, and confiscating VA), and interagency meetings contribute to increasing the level of cooperation among the competent authorities when it comes to investigating and identifying ML crimes.

414. The Coordination Council of the LEAs of the Republic of Uzbekistan, whose decisions are binding for the LEAs, discusses how to increase the effectiveness of anti-crime activities at its meetings.

415. As far as the identification, prevention, and prosecution of predicate crimes and ML is concerned, the LEAs cooperate with each other on a constant basis. All LEAs rated their level of cooperation with the FIU as high.

416. As for international cooperation in the identification and investigation of crimes, it should be noted that apart from international cooperation in the form of MLA, the Agreement on the Procedure for Creating and Running Investigation Groups in the Territory of the Member States of the Commonwealth of the Independent States of 16.10.2015 provides for an opportunity to create joint international investigation groups. However, no such investigation groups were created for ML cases between 2016 and 2020.

417. Officers of the competent authorities are involved in investigative and other procedural activities in the territory of other states during the execution of MLA requests. Although officers of the LEAs were not involved in the investigation of ML cases when MLA requests were executed in other countries.

418. There are statistics and case studies when criminal cases on predicate crimes were sent to prosecute persons who committed crimes in the territory of Uzbekistan and persons who are abroad (Tajikistan and others). No ML criminal cases were received for prosecution purposes or sent for investigation to other states.

419. Overall, the competent authorities have adequate powers and access to electronic databases to gather financial intelligence in order to identify and investigate ML cases and have access to such data.

420. The MIA has access to databases they have, the databases of Interpol, customs and tax information (with the exception of tax secrecy), and a number of others. Information that constitutes tax secrecy is obtained upon request. In terms of information that may be used for financial investigations, the MIA does not have access to data on the registration of small watercraft, and such information is also obtained upon request.

421. The SSS has access to all necessary information.

422. Some databases of the LEAs and other government authorities are integrated into the information systems of the GPO, the MIA, the SCC, and the SSS. If additional information is required, the LEAs use the capabilities of the FIU or send requests to the relevant competent authority.

423. It should however be noted that, in terms of legislation, the preliminary investigation and inquiry bodies and the bodies engaged in OIA received complete access to information that constitutes bank

secrecy only in June 2021 after relevant amendments were introduced into the laws on bank secrecy. Before that, the above bodies had had very limited access to such information. This issue was in part solved by making use of the capabilities of the FIU, but this did not solve the problem in general. Accordingly, the effectiveness of financial (parallel) investigations associated with obtaining bank information could not be high.

424. The internal affairs authorities (MIA) have performed a centralised recording of crimes, including ML, since 2021.[38] Before that, this databank was under the jurisdiction of the GPO. As noted above, the LEAs have different approaches to collecting statistics. In particular, the MIA reports that agency-level statistics did not cover ML crimes, with only predicate crimes being accounted for.

425. There was no recordings of completed financial (parallel) investigations before 2021, i.e. before the joint regulation was adopted. Representatives of the country noted that there was no objective necessity to have such separate recordings because financial (parallel) investigations covered all predicate crimes. The necessity to record completed financial (parallel) investigations is nevertheless obvious given the content of paragraph 4 of the joint instruction of the LEAs[39] concerning the procedure for examining financial aspects of criminal activity when performing OIA, a pre-investigation check, inquiry and preliminary investigation.

426. The country pays significant attention to the training, retraining, and professional improvement of both officers of the LEAs and officers of other authorities that form part of the AML/CFT system.

427. The Academy of the GPO developed relevant AML/CFT training courses, during which 3,085 prosecution employees, 590 employees of the DCEC (operatives, inquirers, and internal auditors), 2,892 employees of the BCE, and 5,393 employees of other ministries, agencies, and organisations underwent training and professional improvement between 2018 and 2020.

Case Study 7.9

The master's degree curriculum at the Academy of the GPO has a speciality in "Anti-Money Laundering and Combating the Financing of Terrorism".

Besides, there is a short-term remote AML/CFT professional development course on "Anti-Money Laundering and Combating the Financing of Terrorism"

428. Relevant professional development training courses in other educational institutions of the LEAs (Academy of the MIA and others) also include the study of ML investigation and identification matters.

429. It is a common practice when the competent authorities prepared information letters concerning their positive experience of identifying and prosecuting ML/TF crimes, identifying new crime typologies, teaching and learning materials, and sending the same to the subordinate structures for information and further use.

Case Study 7.10

To help employees of the DCEC improve their professional skills, including in the area of identifying and solving various criminal schemes involving information technology, the DCEC developed a Guide on the Use of the Public Finance Management Information System (PFMIS) in order to timely identify and prevent the embezzlement of budget funds, tax evasion, and other economic crimes. Analysis based on this Guide revealed more than 500 agreements between 88 business entities and budget organisations that have a "high risk" that economic crimes be committed. Pre-investigation checks and OIM prevented a number of economic crimes related to the improper use of budget funds and tax evasion, and criminal

[38] The procedure for crime registration is governed by the Regulation on the maintenance of a unified information electronic system of criminal statistics, approved by a joint resolution of the GP, SC, SSB, MoI, and SCC dated 30.12.2018, No. KK-83, 08/UM-706-18, 84, 01-02/22-77.

[39] According to paragraph 4 of the joint instruction of the LEAs concerning the procedure for examining financial aspects of criminal activity when performing CIDA, a pre-investigation check, inquiry and preliminary investigation, a financial investigation should be carried out into crimes:

a) that caused especially significant damage or resulted in criminal proceeds in especially large amounts;

b) money laundering, including when a predicate crime is committed outside the Republic of Uzbekistan;

c) that are terrorist in nature, including terrorist financing.

In other cases, a financial investigation should be carried out as decided by the authorised bodies, among other things, prioritising predicate crimes that the NRA identified as having a "very high" and "high" levels of ML risks.

cases were opened.

430. Officers of the LEAs also take part in holding other teaching and learning and research and practical events – conferences, training, discussions of topical AML/CFT matters in the form of roundtables, with practising lawyers, scholars, and international experts involved in this work.

431. The assessors were provided with information that makes it possible to conclude that there are adequate resources (human, physical, information, technical, research and methodological) to ensure that predicate crimes, in general, and ML, in particular, are successfully identified and prosecuted. There is no duplication of powers in the LEAs that would affect the effectiveness and proper allocation of resources. Representatives of the country noted that the turnover of staff in the LEAs is manageable and does not affect the quality of work of the LEAs. As noted above, there are training and professional development programmes for new employees.

432. Given the above, the assessors conclude that in general, the LEAs achieved certain results and have taken some measures to establish systematic work to detect ML, legislation and skills in combating ML have improved, international and inter-agency cooperation has been strengthened.

433. However, the efforts of the LEAs are prioritised on detecting and investigating predicate offences, in frames of which, including through parallel financial investigations, they commonly identify ML. Taking into account that the majority of ML cases are self-laundering and the detection of ML cases by third parties is low, the level of this work is not sufficiently effective.

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

434. During the onsite visit, representatives of the LEAs demonstrated to the assessors that they were sufficiently aware of the NRA and its findings, singling out the main ML threats and risks. They also reported that NRA findings were discussed at various brief meetings in divisions and brought to the notice of employees. Based on the NRA findings, the LEAs, including the FIU, updated their strategic initiatives and plans. In order to ensure prompt responses to changes in ML risks, the MIA and the SCC created specialised situation centres.

435. National anti-crime strategies and minutes of coordination meetings of the LEAs cover AML issues in the context of general anti-crime policy and show that increased efforts are focused on combating predicate crimes that pose very high and high ML risks, in order to, among other things, prevent criminals from generating proceeds that they can later cash out.

Table 7.6. Statistical information about the number of initiated criminal cases into predicate crimes and ML for 2016–2020

FATF designated categories of crimes, Article of the Criminal Code	Level of threat as per the NRA	Total cases	ML cases	%[40]
Corruption and bribery (Articles 167, 205–208, 210–214)	Very high	19,675	112	33.1
Tax crimes related to direct and indirect taxes (Articles 184, 189, 179)	Very high	1,412	106	31.4
Involvement in organised criminal groups (Article 242)	Very high	29	3	0.9
Illegal trafficking of drugs and psychotropic substances (Articles 270–276)	Very high	16,698	2	0.6
Fraud (Article 168 of the Criminal Code)	Medium	33,511	67	19.8
Extortion (Article 165)	Medium	994	4	1.2
Forgery (Articles 209, 228)	Medium	4,394	3	0.9
Environmental crimes (Articles 198, 202)	Medium	150	-	-
Robbery or theft (Articles 164, 166, 169)	Low	32,954	22	6.5
Human trafficking and illegal smuggling of migrants (Articles 135, 223)	Low	1,205	1	0.3
Illegal arms trade (Articles 247–249, 255-1)	Low	1,317	-	-
Money counterfeiting (Article 176 of the Criminal Code)	Low	303	-	-
Kidnapping, false imprisonment, and hostage taking (Articles 137, 138, 245)	Low	147	-	-

[40] As a ratio of the number of ML cases by type of predicate crime and the total number of opened ML crimes.

Smuggling, including in relation to customs and excise duties and taxes (Articles 182, 246)	Insignificant	1,436	16	4.7
Product tampering and counterfeiting (Articles 228-1, 149)	Insignificant	395	-	-
Illegal trafficking of stolen and other goods (Article 171)	Insignificant	76	-	-
Sexual exploitation, including children (Articles 131, 129)	Undefined	4,185	2	0.6
Piracy (Article 164)	Undefined	-	-	-
Insider trading, market manipulation	not criminalised			

436. Analysis of the above data indicated that fraud, theft and robbery, corruption and bribery, and illegal drug trafficking prevail in the structure of crime among the said categories of offences.

437. However, most of the time ML crimes were identified based on tax crimes (including as a result of breaches of the rules of trade) – 31.4%, corruption crimes and bribery – 33.1%, which is consistent with the NRA wherein these acts are assessed as having a very high ML risk.

438. In the NRA fraud was considered to be a medium threat. This assessment isn't consistent with the number of these criminal acts in the structure of crime, the volume of generated proceeds which is the highest figure as compared with other crimes and the number of identified ML facts. During the onsite visit, representatives of the competent LEAs also spoke about the upward trend in the number of fraud cases and criminal proceeds derived therefrom.

439. The ratio between the numbers of crimes involving illegal drug trafficking, the potential volume of generated criminal proceeds, and the number of identified ML facts may indicate that the identification and prevention of ML stemming from this type of predicate crime is not sufficiently effective.

440. Despite a high percentage of theft and robbery in the structure of crime and a large volume of criminal proceeds, the NRA identified these types of crime as having a low level of threat. This assessment is based on the fact that criminal proceeds generated from most of these crimes are insignificant, are not usually laundered, and are used without changing their legal nature for the personal needs of the criminal. However, it is worth noting that the laundering of proceeds generated from these crimes is still not rare.

Case Study 7.11

The investigation found that Mr A committed a theft (UZS 30 million, KZT 1 million, RUB 5 million, USD 26 thousand, other valuables) in especially large amounts by home invasion. Criminal proceeds obtained in the theft were laundered by purchasing three cars in the name of third parties and exchanging the stolen foreign currency for the national one.

Mr B was aware of Mr A's theft but did not report this to the LEAs, and, when aiding Mr A in lending a veneer of legality to the source of the funds obtained during the theft by converting the same into a property, agreeing with Mr A's proposal to register the latter in his name, participated in the purchase of a car worth UZS 47.6 million.

In its judgment, the court found Mr A guilty of theft in especially large amounts, carjacking, illegal purchase of currency valuables, money laundering, and sentenced him to 9 years and 6 months of imprisonment. Mr B was found guilty of concealing the crime, illegal purchase of currency valuables, aiding [Mr A] in money laundering, and sentenced to 5 years and 6 months of imprisonment. The seized three cars, funds, and other valuables were confiscated and forfeited in favour of the victims as compensation for damages.

441. The Supreme Court provided statistical information on the number of persons convicted for ML crimes by predicate crime.

Table 7.7. Statistical information on the number of persons convicted for ML crimes by predicate crime

Types of predicate crimes that preceded ML (Article of the Criminal Code)	Number of persons convicted under Article 243 (ML) of the Criminal Code					Total
	2016	2017	2018	2019	2020	
Corruption and bribery (Articles 167, 205–208, 210–214)	62	26	26	13	18	145
Fraud (Article 168 of the Criminal Code)	24	38	23	33	23	141
Tax crimes related to direct and indirect taxes (Article 184)	37	49	32	8	3	129

Robbery or theft (Articles 164, 166, 169)	26	13	-	2	1	42
Smuggling, including in relation to customs and excise duties and taxes (Articles 182, 246)	10	5	2	2	1	20
Forgery (Articles 209, 228)	4	13	1	-	-	18
Extortion (Article 165)	5	1	-	2	-	8
Illegal trafficking of drugs and psychotropic substances (Articles 270–276)	1	2	1	-	-	4
Involvement in an organised criminal group and racket (Article 242)	2	-	1	-	-	3
Other	3	-	-			3
Sexual exploitation, including children (Articles 131, 129)	1	1	-	-	-	2
Total	175	148	86	60	46	515

442. According to this data, cumulative convictions for corruption crimes and bribery (28.1% of the total number of persons convicted for ML, fraud (27.4%), tax crimes (25%), robbery and theft (8.1%) prevail in the structure of ML-related convictions.

443. The assessors concluded based on these statistics that the NRA may have potentially underestimated the level of threat of theft and robbery.

444. The NRA rated breaches of the rules of trade as crimes with a very high level of ML threat. This conclusion is reasonable given the amount of generated criminal proceeds. The SC reports that in 30 criminal cases the guilty persons were convicted for ML together with breaches of the rules of trade (Article 189 of the CC). It should be noted that a vast majority of such crimes consist in falsifying documents on business transactions and at the same time cashing out of funds. It is not infrequent that cash-out *per se* is an element of an ML typology. Representatives of the country note that this typology relates to ML criminal cases. Non-encashment can be considered as a breache of the rules of trade. The assessors, therefore, believe that it is critical in this specific case to which depth law enforcement officers examine the origin of funds that are cashed out afterwards via falsified trade operations (breaches of the rules of trade). However, it was not possible to make a conclusion on the effectiveness of examinations of financial aspects of activities that preceded cash-out for ML purposes based on available information and case studies.

445. The country nevertheless provided case studies when ML took place and involved other breaches of the rules of trade, for example, non-collection of cash receipts.

Case Study 7.12

A pre-investigation check of the DCEC revealed that Mr M, acting in collusion with other persons, established a legal entity ("M" LLC). Between 2015 and 2016, Mr M, while engaging in trade activities, did not collect trade receipts amounting to UZS 3.3 billion, thereby committing a crime under Article 189 of the Criminal Code (breaches of the rules of trade). A parallel financial investigation into this case revealed that, in order to lend a veneer of legality to the origin of criminal proceeds, Mr M deposited cash amounting to UZS 694 million to increase the authorised fund of "N" LLC. In its judgment, the court found Mr M and his accomplices guilty and convicted them under Articles 189 (Breach of the rules of trade), 243 (ML) of the Criminal Code to various terms of imprisonment.

446. It is characteristic for the country that organised criminal organisations (groups) work there as a means to organise and facilitate the commission of widespread predicate crimes, for instance, drug trafficking, contraband, tax and customs crimes, human trafficking (principally illegal labour migration), forgery of documents, and others. Uniting in OCGs also helps make it easier to launder criminal proceeds.

447. Even though organised crime (Article 242 of the CC – a creation of a criminal organisation) accounts for an insignificant number of ML in statistics, it should be taken into account that the commission of crimes as part of OCGs is also a qualifying criterion in the elements of some highly dangerous crimes. In this case statistics on ML prosecution and judicial examination are reflected by relevant predicate crimes. The identification and investigation of ML crimes as a result of predicate crimes and ML committed by the organised crime is therefore consistent with the level of threat defined in the NRA as high. See Case Study 7.5 for such investigation that is accounted for in statistics of types of predicate crimes.

448. Unlicensed activity is also classified as a crime with a high level of threat in the NRA. However, there was no ML prosecution for these type of crimes.

449. Overall, investigated and prosecuted ML crimes – divided by types of predicate crimes – are consistent with the threats and their levels identified in the NRA, with the exception of fraud, theft and robbery.

450. As for the assessment of the level of consistency of identified, investigated and prosecuted ML crimes with the established levels of ML, the following should be noted.

451. The NRA assessed ML risks as probabilities of ML after a specific predicate crime against potential consequences. Given the above statistics of ML identification, investigation, and prosecution against the predicate crimes that preceded them, it is possible to conclude that the AML practice of the LEAs is consistent with the above assessment of probabilities in the NRA.

452. During the onsite visit, the assessors were provided with information on the most frequently used ML typologies (schemes) and predicate crimes associated with them. However, the list of typologies of most of them contains available practical methods and mechanisms of predicate crimes, i.e. schemes on how to generate criminal proceeds rather than descriptions of further action taken to lend a veneer of legality to criminal proceeds, to conceal their true origin, or to covertly put them into a legal stream of commerce.

453. It was not therefore possible to assess the level of risk as a frequency of use of a specific ML typology (scheme) from a certain category of predicate crime or whether available AML/CFT measures were consistent with them.

454. A state policy of combating corruption and the shadow economy, tax reforms, liberalisation of currency legislation, tax and customs administration, increasing the effectiveness of the LEAs in combating corruption, tax, customs crimes, breaches of trade and service – is generally consistent with NRA findings and aims to increase the effectiveness of measures taken to mitigate ML risks in these areas.

455. In view of the above, the assessors conclude that identified and investigated types of ML in common are consistent with the nature of national threats and risks and national AML/CFT policy. The exception is ML derived from fraud and theft, which, given the overall size of the criminal proceeds generated and the statistics of laundering of such proceeds, is underestimated.

Types of ML cases persued

456. See Table 7.7 for statistics of the Supreme Court of the Republic of Uzbekistan on ML convictions.

457. Courts of the republic try all types of ML criminal cases irrespective of the method of ML, form (self-laundering, with third parties involved, and others) or the category of the predicate crime. As the functions of preliminary investigation and court proceedings are separated from each other and independent in the country, the judicial system cannot influence decision-making relating to the institution of ML criminal cases or referring such cases to court because criminal procedure law prescribes that such matters are to be resolved by the preliminary investigation and prosecution bodies.

458. Given that the number of cases terminated at the investigation stage is insignificant and that other ML cases were received and tried by courts, the assessors conclude that prosecutors represent the state in court, and courts make decisions on various types of ML cases.

Case Study 7.13

Mr A, colluding with bank officials, stole funds from ATMs for two years. Mr A laundered the funds by purchasing movable and immovable property and opening deposits in the name of third parties.
The amount of laundered proceeds reached around USD 160 thousand.
All laundered property was seized during the investigation.
In its judgment, the court convicted Mr A under Articles 167, 243 (ML) of the CC. The bank officials were convicted under Articles 167, 205, 207 of the CC.

The laundered property was forfeited in favour of the state.

459. See Core Issues 7.1–7.2 for other case studies when persons were convicted for various types of ML.

460. Judges do not specialise specifically in ML cases. Cases are assigned to judges by an electronic system with due regard to the judge's workload, experience, and other factors. This mechanism is employed in order to exclude the human factor in the assignment of cases to judges and to ensure that the judges are independent and impartial.

461. According to the approaches existing in the country, ML investigation, it is necessary for the legal establishment of the fact that property was obtained by illegal means (institution of a criminal case or adoption of other procedural decision).

462. During the onsite visit, representatives of the judicial system noted that ML prosecution, as a rule, takes place as part of the prosecution for a predicate crime or after a person was convicted for a predicate crime or after the proceedings on the primary offence were terminated under the non-exonerating reasons.

463. The above approach is statutorily enshrined in Resolution No. 1 of 11 February 2011 of the Plenum of the SC "On Certain Matters of Court Practice in Cases on Money Laundering", paragraph 4 of which states that the court's conclusion that the funds or other property are criminal – and other criminal case files – can be based on a guilty judgment relating to the primary offence, a ruling (decree) on the termination of proceedings on the primary offence for reasons other than exoneration.

464. Thus, even if there is evidence of ML, it is likely that there can be no prosecution for this ML if there is a predicate crime, but no final decision relating to it in the form of a verdict or ruling (decree) on the termination of proceedings in the case for reasons other than exoneration, which the assessors believe to be an aspect that makes ML prosecution and sanctioning more difficult.

465. Relying on the explanations in Resolution No. 1 of 11 February 2011 of the Plenum of the Supreme Court, a predicate crime committed abroad does not prevent prosecution for ML that took place in the territory of Uzbekistan.

466. A single identification of such fact (given the country context of the country, including the prevalence of labour migration of people, the amount of imported cash that exceeds that of exported one, and others) indicates that the level of spread of such types of ML is underestimated. This is due to the fact that, among other things, there are difficulties with identifying and proving that a predicate crime was committed abroad, without which there can be no prosecution for ML in the country.

Table 7.8. Statistics of the Supreme Court on the results of judicial examinations of ML criminal cases (Article 243 of the CC)

Court decision	2016 cases/ persons	2017 cases/ persons	2018 cases/ persons	2019 cases/ persons	2020 cases/ persons
Guilty	90/170	74/146	47/83	31/61	18/46
Acquittal	0/3	3/4	10/25	13/22	14/23
Proceedings terminated	3/3	1/1	0/1	2/2	-
Case remanded for further examination	3/5	1/1	-	-	-
Untried	22/45	23/45	21/35	10/15	12/31
Total cases for trial	118/226	102/197	78/144	56/100	44/100

467. A downward trend in the number of ML cases that courts received to try on the merits is due to a downward trend in the identification of these crimes and the institution of criminal cases under Article 243 of the CC.

468. It should nevertheless be noted that there is a drastic increase in the number of persons acquitted of ML crimes. At the same, time all persons were found guilty of predicate crimes, and there are no acquittals of both ML and predicate crimes.

469. In 2016, the share of the number of acquitted persons was 1.7% of the total number of persons in criminal cases against whom courts adopted final procedural decisions, with this figure being 2.6% in 2017, 22.9% in 2018, 25.9% in 2019, and 33.3% in 2020.

Table 7.9. Information about resentencing under Article 243 of the Criminal Code

Years	Cases retried by higher courts		of which			
			Revoked	of which		Upheld
				Acquitted	Excluded from charges	
	Cases	Persons				
2016	57	77	5	3	2	68
2017	59	93	21	4	3	63
2018	57	85	19	9	6	48
2019	57	79	36	28	8	32
2020	39	70	16	15	1	49
Total	269	404	97	59	20	260

470. The country's judicial system demonstrates principality and impartiality in hearing the ML cases and delivering sentences when it comes to both the need for acquitting accused persons and when there are grounds for sentencing, which also indicates that government measures aimed at ensuring the independence of judges are effective.

Case Study 7.14

The prosecutor's office referred to court a criminal case in respect of Yu.F. and A.A. who used funds they obtained by embezzling government funds by means of appropriation and spending to purchase and register two cars, three residential houses, and a restaurant in the name of third parties in order to launder the funds by concealing the sources of their origin and actual rights.

In its judgment, the court acquitted Yu.F. and A.A. under Articles 243, 167 and convicted them under Articles 184, 189, 228, and other articles of the CC and imposed relevant penalties upon them.

Based on the prosecutor's protest appeal, the court of appeal examined and issued a ruling on revising the judgment of the court of the first instance and found Yu.F. and A.A. guilty under Articles 167 and 243 of the CC too.

The above immovable and movable property was forfeited as compensation for damages and in favour of the state.

471. During the onsite visit, representatives of the judicial system explained that most of the time acquittals in ML criminal cases were delivered as the prosecution bodies were too hasty in opening criminal cases (cases were opened into facts that guilty persons used criminal proceeds derived from predicate crimes with there being no indications of laundering), and it was then established in the court hearing that there were no elements of a crime. As concerns such facts, courts of the republic deliver particular court decrees (special judicial acts intended to rectify breaches of law) that were reported to the LEAs and contained explanations of why there were no indications of ML crimes (Article 243 of the CC).

472. Coupled with a trend in the total number of identified ML crimes, considerable growth in the number of acquitted persons, as well as the number of ML-related verdicts revised by higher courts, supports the assessors' conclusions that the effectiveness of work of the LEAs in the area of identifying and investigating ML crimes requires improvement.

473. According to criminal procedure law, public prosecutors are entitled to drop charges which results in the proceedings being terminated by the court. However, the GPO reports that there were no cases when public prosecutors dropped charges in ML cases over the period in question. In view of this, as there were acquittals for ML and as prosecutors did not revoke hasty rulings on the institution of ML criminal cases, the effectiveness of the prosecutor's supervision over the prosecution bodies also requires improvement.

474. The Higher School of Judges, whose curricula also cover AML/CFT/CPF matters, helps judges improve their professional skills.

475. Accordingly, the assessors conclude that the organisation of judicial examinations of ML cases largely ensures an impartial and objective consideration of any type of ML cases, except when there

is no conviction for a predicate crime or there is a decision to terminate a case on a predicate crime for reasons other than exoneration. The downward trend in the number of ML cases and the increasing number of acquittals is not due to inefficiencies in the judicial system, but to the shortcomings highlighted in Core Issue 7.1.

Effectiveness, proportionality and dissuasiveness of sanctions

476. The country's criminal law classifies ML as a grave crime. Article 243 of the CC provides for a sanction in the form of imprisonment for 5 to 10 years. There are no additional types of punishment under Article 243 of the CC, and the sanction imposed by this article has no alternative.

477. However, sanctions for predicate acts similar in purposes to ML (e.g., tax evasion, breach of customs law, illegal business activity, breach of the rules of trade, and others) provide for punishment in the form of a penalty, corrective labour, and restriction of freedom.

478. Additionally, the disposition of Article 243 of the CC does not establish qualifying criteria of the act, implying that it does not allow ranking liability depending on the amount of laundered property and in cases when a crime is committed by a special subject (an official, a person previously convicted for a similar crime, persons of an organised group, and others)

479. As explained in Resolution No. 1 of February 3, 2006, of the Plenum of the Supreme Court "On Court Practice of Criminal Punishment", punishment should be just, i.e. it should be imposed individually in each case, consistent with the nature and level of public danger of the crime, the personality of the guilty person, and aggravating and mitigating circumstances.

480. According to Resolution No. 1 of February 11, 2011, of the Plenum of the Supreme Court, when imposing punishment under Article 243 of the CC, courts should take into consideration the amount of laundered property.

481. Sentences for ML crimes are delivered only together with convictions for predicate crimes. As per the rules of Article 59 of the CC, in such cases punishment is imposed on a separate basis for each crime and then finally for the totality of crimes in the following ways: i) a more lenient punishment is absorbed by a more severe one; ii) imposed punishments are cumulated in part; iii) imposed punishments are cumulated in full.

482. The punishment for the predicate crime largely influences the term of the final punishment for the totality of crimes. However, the punishment for ML also influences the final punishment.

Case Study 7.15

In its judgment, the court found Mr S guilty of crimes under Articles 243 of the Criminal Code (ML), Articles 28, 246 of the CC (Organisation of contraband), Article 273 of the CC (Illegal drug trafficking, including the sale of drugs), Articles 25, 273 of the CC (Preparation for (attempt at) illegal drug trafficking). The following punishments were imposed upon him: under Article 243 of the CC – 5 years of imprisonment, under Articles 28, 246 of the CC – 11 years of imprisonment, under Article 273 of the CC – 13 years of imprisonment, under Articles 25, 273 of the V – 11 years of imprisonment. In the end, according to Article 59 of the CC, he was sentenced to 14 years of imprisonment for the totality of crimes after his punishments were cumulated in part.

Table 7.10. Statistics on punishments under Article 243 of the Criminal Code imposed by courts

Indicator	2016	2017	2018	2019	2020
Sentences delivered	85	70	64	50	
Persons convicted	169	136	110	86	
a) punishment in the form of imprisonment	154	111	85	72	
5 years	79	86	59	41	
6 years	41	17	14	18	
7 years	12		5	6	
8 years	8	6	4	3	
9 years	5	2	3	2	
10 years	1			1	

b) punishment imposed with the application of Article 57 of the Criminal Code	23	25	25	14	

483. However, it is worth noting that courts widely apply the provisions of Article 57 of the CC, i.e. imposing punishment below the lowest threshold of the sanction under Article 243 of the CC or a lenient punishment.

484. According to law, Article 57 of the CC is applied in exceptional cases involving circumstances that considerably reduce the level of public danger of the crime.

Table 7.11. Information about the application of Article 57 of the CC in criminal cases opened under Article 243 of the CC in correlation with the application of the above provision for predicate crimes to ML (in relation to convicted persons for the totality of the predicate crime and ML)

By year	Number of convicted persons	In relation to convicted persons with the application of Article 57 of the Criminal Code		Application of Article 57 of the Criminal Code in relation to convicted persons, as a percent	Share of the application of Article 57 of the Criminal Code between 2016 and 2020
		Article 243 of the Criminal Code	Predicate crimes		
2016	175	13	36	7.4	14.3
2017	148	23	31	15.5	25.3
2018	86	27	18	31.4	29.7
2019	60	16	18	26.7	17.6
2020	46	12	8	26.1	13.2
Total	515	91	111	17.7	20.2

485. Representatives of the SC noted that the widespread application of Article 57 of the CC is down to the fact that the sanction under Article 243 of the CC has no alternative and does not allow ranking the liability of guilty persons depending on the circumstances of the crime (duration of criminal activities, amount of laundered proceeds) and data on personality (e.g., dependent children, health status, and others).

486. Representatives of the SC also noted that, in practice, when courts convicted persons under Article 243 of the CC with the application of Article 57 of the CC, they imposed more lenient types of punishment rather than sentencing them to imprisonment below the lowest threshold of the sanction.

487. That there is no proportionality of ML-related sanctions, i.e. that they are inconsistent with the public danger of crimes, compels the judicial system to impose a more lenient punishment in a large number of criminal cases.

488. No persons who previously committed crimes under Article 243 of the CC were convicted for ML over the period in question.

489. Uzbek law does not provide for criminal and administrative liability of legal entities. According to laws, civil and legal liability includes an ability to wind up (dissolve) a legal entity. However, this liability for ML was not applied to legal entities in practice.

490. With that said, the assessors conclude that the country does not apply sanctions against legal entities for ML.

491. Although the sanctions provided by criminal law are not proportional, the courts ensure proportionality by applying article 57 of the CC. At the same time, in accordance with the principles of criminal law, the most severe punishment - imprisonment - is imposed in cases where the application of milder measures is not sufficient to correct the perpetrator and prevent new crimes. Accordingly, the practice of imposing sentences for ML in Uzbekistan is dissuasive and proportionate.

Use of alternative measures

492. The assessed country noted that if indications of ML are not proven, a person is prosecuted and convicted for a predicate crime in practice.

Case Study 7.16
Five Cameroonian nationals took possession of funds (USD 100 thousand) of an individual by fraudulent

means.
The investigation received information that they laundered some of the stolen funds by purchasing movable and immovable property in Cameroon that was fictitiously registered in the name of third parties.
Replies of 11 foreign states to the FIU's requests through the Egmont Group did not make it possible to support the case for laundering.
As there was no evidence of guilt of ML, the guilty persons were held criminally liable and convicted for fraud (Article 168 of the CC).

Case Study 7.17
Mr K and Mr U, as part of a group of persons acting by precious concert, in order to take possession of another's property by false pretences, promised Qatar nationals to organise an illegal hunt in the territory of the Republic of Uzbekistan for a certain amount that the former wanted to be credited to accounts in foreign banks. However, the LEAs disrupted their activity.
A criminal case was opened in this regard against the above persons under Articles 25, 168 of the CC (attempted fraud).
No ML criminal case was instituted because the crime was prevented before criminal proceeds were derived and there was no objective evidence of the guilty persons' intention to launder the money.

493. Representatives of the GPO noted during the onsite visit that, as an alternative, consideration is now given to the identification of other elements of crimes (such as the purchase or sale of criminal property; entering into a transaction contrary to the interests of the Republic of Uzbekistan; false business; evasion of tax and customs payments; illegal business; breach of the rules of trade or service; neglect of official duty, and others)

494. The assessors note that criminal liability for the above crimes can be considered as alternative measures in lieu of ML prosecution. However the country did not provide any digital data and case studies when ML prosecution was initiated but, in the same case, the person was later accused of other elements of a crime.

495. It was not therefore possible to reach conclusions as to the extent of influence of this alternative measure in practice in the absence of a real prospect of ML conviction.

496. No examples of other alternative measures to conviction for ML were provided.

Overall conclusions on IO.7

497. The LEAs have achieved some results and make attempts to establish systematic work to identify and investigate ML, legislation and skills in combating ML are being improved, and international and inter-agency cooperation is being strengthened.

498. However, the efforts of the LEAs have focused on detecting and investigating predicate offences. Given that most cases of ML are self-laundering and the detection of ML by third parties is low, the level of this work is not sufficiently effective.

499. The types of ML detected, investigated and prosecuted are generally consistent with the nature of national threats and risks and national AML policies, except for ML arising from fraud and theft, which, given the overall size of the criminal proceeds generated and the recorded cases of ML, are probably underestimated in the NRA.

500. The investigation and prosecution of ML are likely complicated by the need for a final judgment on the predicate offence in the form of a sentence or dismissing the case under the non-exonerating grounds.

501. Physical persons convicted of ML offences are primarily subject to proportionate and dissuasive sanctions. Sanctions against legal persons are not applied.

502. Where ML is not proven, prosecution and conviction for a predicate offence are practised.

503. **The Republic of Uzbekistan is rated as having a moderate level of effectiveness for IO.7.**

Immediate Outcome 8 (Confiscation)

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

504. One of the priorities of the state's policy in the field of combating crime is compensation for damage caused by a crime. In accordance with Article 82 of the CPC, the nature and extent of the harm caused by the crime are one of the circumstances to be established during the inquiry and preliminary investigation. However, the CPC does not contain regulations identifying the property obtained by criminal means or income obtained as a result of the use of such property as the circumstances to be proven in a criminal case.

505. The adoption of measures to ensure the execution of sentences in terms of property and other penalties, the completeness of compensation for damage caused are the criteria for evaluating the effectiveness of investigative units (Resolution of the CM No. 727 of 15.09.2017, Order of GPO No. 131 of 29.06.2016). The actual execution of sentences in terms of penalties in favour of the state, individuals and legal entities, along with other indicators, determines the assessment of the effectiveness of the activities of state enforcement officers (Order of the BCE No. 63 of 08.08.2019).

506. The national policy in the field of AML/CFT/CPF is determined by the Strategy for the Development of the National System of the Republic of Uzbekistan for countering the legalization of proceeds from crime, financing of terrorism and financing of proliferation of weapons of mass destruction, approved by Presidential Decree No. UP-6252 dated 06.28.2021 (hereinafter Strategy). The documents that determined the national policy on the matter under consideration before the Strategy approval were not provided to assessors.

507. The Strategy defines the priorities of the state in the field of AML/CFT/CPF activities and mechanisms for their implementation, including strengthening cooperation with foreign states in the areas of search, arrest, confiscation and return of property obtained from criminal activity and assets from abroad.

508. The legislative definition of the concept of "confiscation" is fixed in the CC, the procedure for the application of confiscation is regulated by the law rules of the CPC. The CC does not contain the concept of "confiscation" therefore, confiscation is not an institution of criminal substantive law. This gap in legal regulation allowed assessors to conclude that confiscation is not considered as a legal consequence of the crime commission, a measure of criminal justice and legal enforcement action applied to a perpetrator and a purpose of law enforcement agencies and the judicial system in their implementation of prosecution and justice.

509. The correction to the law regarding statutory regulation of confiscation is not stipulated in the Decree of the President of the Republic of Uzbekistan dated 14.05.2018 No. PP-3723 "On measures to radically improve criminal and criminal procedure legislation" and the Concept of improving criminal and criminal procedure legislation, as well as the Roadmap for implementation of the tasks defined in the Strategy.

510. The confiscation of criminal proceeds is based solely on criminal procedural mechanisms. The basis for the application of confiscation is the implementation of criminal prosecution. The country's legislation does not contain a mechanism for the application of confiscation outside the framework of criminal prosecution (for example, the confiscation of unexplained proceeds of officials within the anti-corruption law), as well as its application when criminal prosecution cannot be performed (for example, when a criminal has disappeared and is on the wanted list).

511. The country has taken measures to intensify the activities of LEAs to identify and trace the proceeds of crime, funds for the financing of terrorism, targets of crimes and other assets, including a property of equivalent value, which may be subject to forfeiture to the state's revenue. Specifically, in 2021, joint guidance of the GPO, the SSS, the MIA and the SCC on the procedure for examining the financial aspects of criminal activity at the stage of pre-trial proceedings was approved, amendments and additions were made to Resolutions of the Plenum of the SC No. 1 of 11.02.2011 "On certain issues of judicial practice in cases of legalization of criminal proceeds", No. 26 of 27.12.2016 "On

judicial practice on the application of legislation on compensation for property damage caused by crime", as well as to some GPO's orders.

512. Resolution of the Coordinating Council of LEAs of the Republic of Uzbekistan dated 30.04.2021 states that the inquiry and preliminary investigation units are obliged to use all the powers and mechanisms provided by law in order to identify and arrest the criminally acquired property. Considering the assessed period (2016–2020), these (and other) regulations were considered when assessing technical compliance but did not affect the conclusions on effectiveness.

513. Thus, compensation of property damage caused by the crime (restitution to victims) is considered as the main task of the state's policy in the field of combating crime. Confiscation of criminal proceeds is applied when the person who suffered property damage is not identified or when a criminal property is not subject to return to a victim (for example, a bribe), or with respect to the property exceeding the amount of damage from crime.

514. The analysis of regulations of government departments demonstrated that prior to the introduction of appropriate amendments and additions, the efforts of LEAs were focused on ensuring compensation for property damage from crimes. However, material damage caused by crime and income obtained by criminal means are not always recognized as identical concepts. For example, such crimes as drug trafficking, arms trafficking, illegal migration, and sexual exploitation do not usually involve property damage, but generate criminal proceeds.

515. Considering the above-mentioned legal considerations of confiscation, assessors conclude that the confiscation of criminal proceeds from crimes not related to causing material harm, confiscation of instruments and means of committing crimes and property of equivalent amount for the purpose of their forfeiture to the state’s revenue is not a purpose or a mechanism for the implementation of state policy to combat crime.

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

516. In order to identify and trace criminal proceeds, instruments and means of crime, other assets, including the property of equivalent value, seizure to ensure material damage and confiscation of property (see the detailed analysis on Recommendation 4), LEAs conduct parallel financial investigations.

517. The joint resolution of the GPO, MIA, the SSS and the SCC (2021) establishes that conduct of a parallel financial investigation is mandatory, based on the facts of crimes: a) that caused especially large damage or large-scale criminal proceeds; b) legalized income from criminal activity, including when the offence was committed outside the country; c) have a terrorist nature, including the financing of terrorism.

518. In other instances, the priority in the decision of the competent authority to conduct a parallel financial investigation is given to predicate offences classified under the NRA as having a very high and high risk of ML. As noted in IO 7, the representatives of the LEAs indicated that prior to the adoption of the above-mentioned interdepartmental regulatory act, parallel financial investigations were conducted for all predicate offences. However, statistical data to support these arguments are not provided due to the lack of such records.

519. According to the information provided, in criminal cases of predicate offences investigated by LEAs in 2016–2020, the amount of property damage caused by crimes was 8,625 billion UZS (about $811 million), thereat the proceeds from crime were 8,241.4 UZS ($775 million). The damage in ML criminal cases amounted to 1,848 billion UZS ($173.8 million), including criminal proceeds of 650.9 billion UZS ($61.2 million).

520. A distinctive feature of the country is a high level of voluntary compensation by perpetrators of material damage, criminal proceeds for the assessment period, 81.1% of the total material damage was voluntarily compensated, including 64.2% of the damage caused by ML crimes.

Table 8.1. Information on the amount of damage voluntarily reimbursed

Year	GPO	SSS	MIA	Total
	voluntarily paid, returned to the victim	voluntarily paid, returned to the victim	voluntarily paid, returned to the victim	voluntarily paid, returned to the victim
2016	189,6	13,6		203,2
2017	39,4	7,8	0,1	47,3
2018	749,0	20,6		769,6
2019	132,0	5,7		137,7
2020	25,3	3,5		28,8
Total	1 135,3	51,2	0,1	1 186,6

521. The high ratio of voluntary compensation for property damage is due to the presence in the criminal law of the country of certain norms that encourage perpetrators to positive post-criminal behaviour. Specifically, the voluntary compensation for damages in certain categories of crimes may entail exemption from criminal liability or punishment; non-application of the most severe types of punishment to the offender in the form of personal restraint and imprisonment or restriction of the type or imposition of a sentence of no more than 2/3 of the maximum penalty established for the crime.

522. Full compensation for damages in the form of taxes and other mandatory payments, including penalties and financial sanctions accrued based on the results of a tax audit, entails unconditional exemption from criminal liability of persons who have committed tax evasion for the first time.

523. Thus, the provision of compensation for property damage from crimes, proceeds of crime, is carried out to a greater extent through the application of criminal justice encouragement, entailing voluntary compensation for harm by perpetrators, and not solely through the exercise by LEAs of their procedural powers to take interim measures. Assessors considered the effectiveness of the norms in Uzbekistan that encourage positive post-criminal behavior of the perpetrators for the purposes of confiscation. However, voluntary reparation of harm and payment of criminal proceeds should not be considered by the competent authorities as a circumstance exempting them from the need to perform the functions of identifying and seizing the property subject to confiscation.

524. In order to ensure compensation for damage, confiscation of criminal proceeds during the preliminary investigation of predicate crimes, the property of a total value of 1,461.6 billion UZS ($137.4 million) was seized by LEAs, which amounted to 89.7% of the damage that was not voluntarily compensated by perpetrators. Representatives of the LEAs pointed out that interim measures in the form of arrest are not always possible due to the low level of material wellbeing of perpetrators and their lack of property. This argument has been considered to a certain extent by assessors, but in general, this indicator shows that the work of the LEAs to identify and seize property in criminal cases of predicate offenses needs to be intensified and improved.

525. In criminal cases of ML crimes, the competent authorities have demonstrated increased efficiency. In such criminal cases, property with the value of 826.9 billion UZS ($77.7 million) was seized, while the amount of damage not voluntarily reimbursed amounted to 661.4 billion UZS ($62.2 million). Thus, the value of the seized property significantly (by 25%) exceeds the amount of non-reimbursed damage, which indicates the effectiveness of the interim measures applied in the cases of ML crimes.

526. The country provides examples of the identification and seizure of property in significant amounts.

Case Study 8.1. (Seizure of property)

During the pre-investigation check carried out by the DCEC, the facts of embezzlement of 8.5 million USD of budget funds were established.

The stolen funds were legalized through the purchase of 110 cars, 40 apartments and other real property items that are fictitiously registered as the ownership of third parties.

Criminal cases have been initiated against the official and 12 accomplices under articles 167 (embezzlement by appropriation), 205 (abuse of power or official authority), 209 (forgery in public office) and 243 (ML) of the CC. During the preliminary investigation, the damage in the amount of 5.1 million USD was voluntarily compensated, property worth 4.7 million USD was seized. The criminal

case was sent to the court for consideration on the merits.

Table 8.2. Information on the seizure of property in ML criminal cases (Article 243 of the CC) investigated by the units of the prosecutor's office is given in the table below (millions of USD).

No.	ML criminal cases	2016	2017	2018	2019	2020	Total
1	Number of cases	77	74	63	29	27	270
2	Legalized	71.8	13.5	114.3	28.8	4.9	233.3
3	Voluntary compensation is provided	57.1	11.3	33.5	2.4	1.4	105.7
4	Seized property	10.2	0.8	58.5	13.4	1.3	84.2
5	Total	67.3	12.1	92	15.8	2.7	189.9

527. Thus, the prosecutor's office imposed a freezing order on the property valued at 81.4% of the value of legalized criminal proceeds, which is quite a high indicator.

Case Study 8.2. (Identification of property subject to seizure in the course of a parallel financial investigation)
During the investigation by the prosecutor's office of the criminal case against Yu., it was established that he, working as a deputy head of the department, acting upon preliminary collusion with 4 officials, received the money in the amount of 4.3 million USD as bribes for creating favorable business conditions for several business entities, and also committed embezzlement of budget funds in the amount of 16 thousand USD.
Using the funds obtained from crime, Yu. created several companies fictitiously registered in the names of third parties, acting as a leader of which he committed a violation of trade rules and service provision rules, tax evasion totalling 655,000 USD. In cooperation with the DCEC and the MIA, a parallel financial investigation was conducted, which established that criminal funds of 2.7 million USD were legalized by Yu. legalized through the acquisition of 9 real estate assets and 10 premium cars fictitiously registered as the property of third parties.
The property worth 3.8 million USD was seized. Yu. and his accomplices were found guilty by the court of taking bribes, embezzlement by appropriation, money laundering, and other crimes and sentenced to various terms of imprisonment. The seized property was used to pay off property damage, and the remaining part of the property was confiscated to the state's revenue.

528. The SSS provided information on the seizure of property in ML cases, broken down by property type. In the period of 2016–2020, the investigative units of the SSS issued freezing orders on real property (with a total value of 79.2 billion UZS), motor vehicles (UZS 5.4 billion), other valuables (UZS 12.3 billion), cash in national currency (UZS 29.4 billion), USD ($4.8 million), Russian rubles (7.1 million rubles), Kazakh tenge (24 million tenges).

Case Study 8.3. (Identification and confiscation of criminal proceeds from illegal drug trafficking)
In the criminal case against H., J. and M. it was established that they organized the smuggling of drugs from Tajikistan and their illegal sale in the Republic of Uzbekistan. Part of the funds received by the perpetrators from illegal drug trafficking was legalized by purchasing movable and immovable property fictitiously registered as the property of third parties.
In the course of a parallel financial investigation, the following assets were identified and seized: 12.5 thousand US dollars, 3 real estate assets worth 111 million UZS (about 10.5 mln USD) and a car.
These persons were found guilty by the court of smuggling, illegal trafficking of narcotic drugs and ML and sentenced to long terms of imprisonment. The property and funds seized during the investigation were confiscated and forfeited to the state's revenue.

529. In ML criminal cases investigated by the MIA investigative units during 2016–2020, the amount of material damage caused by predicate offenses amounted to 191.3 billion UZS; the amount of legalized funds is 60.8 billion UZS. The assets worth UZS 126.8 billion were seized, which amounted to 66.3% of the damage caused.

Case Study 8.4. (Identification and confiscation of criminal proceeds obtained as a result of fraud)
M., having organized LLC "E" by creating a financial pyramid under the pretext of returning the received assets (money, real estate, vehicles, etc.) in a twofold amount, fraudulently took possession of

funds in the amount of 29 million USD, vehicles, and real property worth UZS 20 billion, belonging to 6,636 persons.
The stolen funds were legalized by M. through the acquisition of 18 real estate assets, 85 vehicles and other property fictitiously registered as the property of third parties. During the parallel financial investigation, the legalized property assets were identified and seized. According to the court verdict, M. was found guilty of fraud and ML. The seized property was forfeited by the court to compensate the victims.

530. The above data allowed assessors to conclude that when carrying out criminal prosecution, LEAs actively use the procedural powers granted to them to seize property as a measure ensuring subsequent compensation for material damage, confiscation of property, however, the work in this area of activity needs to be improved.

531. The legislation of the Republic of Uzbekistan regulates the mechanisms of management of seized and confiscated property assets, depending on the property type. The LEAs demonstrated knowledge of the relevant law rules, provided practical examples of managing complex assets (a manufacturing facility), which made it possible to prevent the shutdown of its activities.

532. In 2021, a joint resolution of the GPO, MIA, SSS and the SCC approved the procedure for the freezing, storage and confiscation of crypto-assets. This interdepartmental document defines an algorithm for identifying by LEAs the information on the circulation of VAs. VA are subject to freezing and attachment until their origin is clarified and/or a court decision is made. The arrest is carried out by transferring VA to the crypto wallet of the LEA. Thereat, the value of crypto-assets is determined at the time of withdrawal according to cryptocurrency exchange quotes, for non-convertible assets – in accordance with the prices on financial service platforms. Confiscation and forfeiture of VAs to the government are carried out in accordance with the exchange (sale) procedure established by law.

Case Study 8.5. (Confiscation of crypto-assets)
According to the court verdict of 26.11.2020, T. who illegally sold 9.5 bitcoins for 224,000 USD, was found guilty of committing crimes proscribed under part 4 of article 177, par. "a" (illegal purchase or sale of currency valuables) and article 190, part 2, par. "a" (activity without a license) and sentenced to punishment in the form of a fine in the amount of 300 RSV or 66.9 million UZS. Crypto-assets were confiscated to the state's revenue.

533. Thus, the country has demonstrated the fact of successful identification, seizure and confiscation of VA that were the target of a crime, to forfeit them to the state. However, according to the information received from the representatives of BCE by the experts during their on-site mission, the court's verdict regarding the realization of crypto-assets is in progress.

534. The existence in the country of a mechanism for identification, seizure and confiscation of VA is a necessary tool in implementing the tasks of identifying and suppressing potential ML cases committed through the use of such assets.

535. The tax authorities conduct audits to check compliance with tax legislation. If they identify any violations, the materials of tax control measures are transferred to the DCEC to conduct a legal assessment for establishing the corpus delicti. Total for the period 2016–2020 STC sent 5,830 materials to the FIU, based on which 1,275 criminal cases were initiated. In addition, 1,453 materials of tax authorities were entered as evidence in the files of criminal cases, including for the purpose of establishing the amount of criminal income. The above information, as well as data on the collaboration of the STC with other LEAs (see the detailed analysis related to the IO 5 performance), indicate its effectiveness in contributing to the timely detection and suppression of tax crimes, the seizure and confiscation of criminal proceeds from the perpetrators.

536. According to the information provided by the SC of the Republic of Uzbekistan, in criminal cases considered in 2016–2020, the criminal proceeds from predicate offenses amounted to 6,520,079.3 million UZS (about $613 million). In this regard, the crimes generating the highest income were

fraud, corruption and bribery, tax crimes, and smuggling. The material damage caused by crime does not substantially exceed the criminal proceeds and amounted to 6,675,792.8 million UZS.

537. The amount of legalized criminal proceeds in the ML cases considered by the courts amounted to 1,000 949.5 million UZS ($94.1 million), while the largest share is legalized income obtained from tax crimes, corruption crimes and bribery, fraud, smuggling.

538. The above data are consistent with the NRA in terms of attributing tax and customs crimes, corruption and bribery to the criminal acts with a very high degree of ML threat and do not fully correlate with the NRA assessment of fraud as a medium-degree risk.

539. Compensation for material damage caused by crimes, when it is not paid on a voluntary basis, is carried out through the civil lawsuit institution in criminal proceedings. A civil claim may be brought against the guilty person by an individual or legal entity, who has suffered harm from a crime, as well as by a prosecutor.

540. In 2017–2020, the courts considered more than 21,000 civil claims, for which 3 959.2 billion UZS were recovered to compensation for material damage caused by crimes (about $372 million).

541. In the cases established by law (in the absence of the grounds for restitution to victims), the courts decided to confiscate the proceeds obtained by criminal means, the instruments and means of committing a crime, the monetary equivalent of criminal income.

542. According to the data of the SC for 2016–2020 on predicate offenses there were court decisions on the confiscation of property worth 98.5 billion UZS ($9.3 million), including instruments of crime worth 3.2 billion UZS ($299,700), objects of crime with a total value of 28.6 billion UZS ($2.7 million), other objects (things) – 66.7 billion UZS ($6.3 million). Information on the volume of confiscation in the terms of predicate offenses is not provided. Thus, in relation to the amount of obtained proceeds from crime, the volume of confiscation by courts is insignificant (9.9% of the total amount of received criminal proceeds was recovered). This indicator is explained by the significant amount of voluntary compensation and the priority of compensation for damage over a confiscation measure.

543. In ML criminal cases (Article 243 of the CC) considered during the analyzed period, the decisions on compensation for material damage caused by crimes were made by the courts for 70 cases, the decisions on recovery of monetary equivalent of criminal proceeds – for 113 cases, on confiscation of instruments of crime – for 47 cases. Information on the confiscation amount (recovered amounts) in criminal cases of ML crimes is not provided.

544. The country provides examples of the recovery of monetary equivalent (however, no information is provided on the amount of recovery in such exemplified cases).

Case Study 8.6. (Recovery of monetary equivalent)
According to the court verdict N. was found guilty of incitement to bribery, fraud and other crimes and sentenced to imprisonment.
The court found that N., acting upon preliminary collusion with another person, having gained the trust of G., received from the latter 6,000 USD to transfer as a bribe to officials of a higher educational institution for admission to study, this sum he seized and disposed of at his discretion. The value equivalent of the subject of the bribe was charged from the convicted person and collected to the state's revenue.

545. According to Article 284 of the CPC, upon the termination of proceedings in a criminal case, the confiscation of property of an equivalent value is carried out by a court in civil proceedings.

546. In accordance with Order of the Prosecutor General of the Republic of Uzbekistan No. 129 of 22.02.2016 "On the efficiency of ensuring the rule of law and the protection of individual rights and freedoms in the fight against crime, in the conduct of the inquiry, preliminary investigation and criminal intelligence operations" (as amended by Order No. 226 of 19.04.2021) prosecutors are obliged, when terminating criminal cases relating to the ML and TF, to resolve the issue of confiscation of money and other property obtained from crime by filing a claim in court.

Table 8.3. Information on the number of civil lawsuits brought by prosecutors upon termination of criminal cases and the amount of funds recovered.

No.	Civil lawsuits of prosecutors	2016	2017	2018	2019	2020	Total
1	Number of claims	53	25	22	26	13	139
2	Amount recovered (thou. USD)	200.4	125.6	184.3	179.9	64.7	754.9

547. These data indicate that prosecutors exercise the procedural powers granted to them and seek to recover criminal proceeds upon termination of criminal prosecution.

Case Study 8.7. (Recovery of monetary equivalent in civil proceedings in connection with the termination of criminal prosecution on non-exculpatory grounds)

R. and M., acting under the false pretense of offering to give a bribe to an employee of the internal affairs unit, not intending to fulfil their obligations to transfer a bribe, took possession of X's funds in the amount of 3,700 USD.

The criminal case under Articles 168 (fraud) and 211 (incitement to bribery) of the CC was terminated by the criminal prosecution unit on the basis of an amnesty act. The funds that were the subject of the bribe were not compensable to the victim. According to a court decision, the prosecutor's claim was satisfied in civil proceedings, the criminal proceeds recovered in the full amount from R. and M. were forfeited to the state's revenue.

Case Study 8.8

A. and B. by inciting to bribery, fraudulently took possession of S.'s funds in the amount of 11,800 USD, promising the latter to transfer the money as a bribe to officials, and subsequently spent the money on their own needs.

Pursuant to the court verdict, A. was sentenced to imprisonment. 11,800* USD were collected from him to the state's revenue.

The criminal case against B. was terminated on the basis of an amnesty act. According to the Prosecutor's claim, considering the receipt of criminal proceeds by both perpetrators, the court in civil proceedings resolved to recover 11.800 USD from A. and B. on a basis of solidary liability.

548. Enforcement of court decisions regarding the recovery of material damage, confiscation of property, fines falls within the competence of the BCE. When performing its functions, the BCE is not limited to the property identified at the stage of criminal prosecution, investigating the debtor's property status to the full extent. If the property assets that had not been found earlier are identified at the stage of execution of the sentence, such property is subject to seizure and forfeiture to compensate for damages or confiscation. For 2018–2020 The BCE seized the property of the persons convicted of predicate offenses in the amount of 4.1 billion UZS.

549. According to the statistical data provided by the BCE, in 2016–2020, the amount of 7,170,834 million UZS was collected to compensate for material damage according to executive documents ($1,656.9 million), the cash funds and other property totalling 2,388,375 million UZS ($416 million) were forfeited to the state's revenue.

Table 8.4. Information on the criminal proceeds actually confiscated according to enforcement documents (in USD).

Period	Proceeds	Crime instruments	Equivalent
2016	1,804,823	1,260,834	2,460,239
2017	7,209,304	1,470,363	5,779,952
2018	1,248,681	806,048	1,241,709
2019	2,997,373	728,460	1,094,358
2020	17,547,380	439,008	117,423
total	30,807,561	4,704,713	10,693,681

550. BCE for 2016-2020 actually recovered 71.9% of the recoverable amount of property damage caused by crimes (restitution to victims), and transferred 77% of money and other property to the state’s revenue (confiscation).

551. Assessors considered the country's arguments that the actual enforcement of court decisions in 2020 was significantly hindered by the measures taken to prevent the spread of coronavirus. However, there has been a definite downward trend in the real enforcement of court decisions before. For example, while in 2016 and 2017 BCE actually seized 92.6% and 93.4% of the property and funds to be converted to state revenue, in 2018 the figure was only 77.1%. Considering that the effectiveness of confiscation is ultimately determined by the actual execution of a court decision efforts taken by enforcement authorities need to be enhanced.

552. The procedure for distribution of the funds received from the sale of property forfeited to the state's revenue is determined by Resolution No. 200 of the CM dated 15.07.2009, which sets out (upon the expropriation of the confiscated property by relevant authority) the transfer of 16% to each of the SSS and the special fund for incentive funding of the customs service and border guards, 10% – to the DCEC, and 8% of the money received from the sale of all types of property are put at the disposal of the Court and Justice Development Fund.

553. The country takes measures to identify and seize criminal assets transferred abroad. In 2016–2020, prosecution authorities sent 24 requests to foreign countries for mutual legal assistance in the field of search and seizure of assets, 20 of them were executed. In total, in response to the country's requests, property worth more than 800 million USD was seized in foreign countries.

554. The confiscation of proceeds transferred to other countries and the return of assets was made in one criminal case (see below).

Case Study 8.9. (Confiscation of proceeds transferred to other countries and return of assets)
An organized criminal group, which included 11 citizens of the Republic of Uzbekistan, committed theft of state property in the amount of 35 million USD. In order to legalize criminal proceeds with the help of foreign citizens (professional money launderers), the stolen funds were withdrawn to the accounts of offshore companies, subsequently used to acquire assets in the form of business entities, shares, movable and immovable property in European countries, and part of the stolen money was placed on bank deposits and in safety deposit boxes.
During the preliminary investigation, criminal assets of the organized criminal group abroad were identified, including real properties in France worth 10 million USD, in the Russian Federation worth 90.1 million Russian rubles, funds in Switzerland (335 million USD), which were seized by the competent authorities of foreign states at the request of the Republic of Uzbekistan for mutual legal assistance.
The participants of an organized criminal group were convicted of corruption crimes, embezzlement, and ML and sentenced to imprisonment by a court verdict. The seized property was decided to be forfeited to the state's revenue. As a result of the work carried out by the GPO with other state agencies for the sentence execution, criminal assets located in France were sold and received funds in the amount of 10 million USD were returned to the Republic of Uzbekistan. The work is ongoing for confiscation of assets of organized crime groups and return from other countries.

555. The single fact of the identification and return of assets from abroad was explained by the representatives of the LEAs by the fact that in the vast majority of cases both the disposal of criminal proceeds and their legalization are carried out in the territory of Uzbekistan (as a rule, by acquiring movable and immovable property assets with their fictitious registration with the aim of laundering and transfer to third-party ownership). However, assessors concluded that LEAs do not pay due attention to the search and return of assets from abroad and their work in this area of activity needs to be intensified.

556. Requests from foreign countries for property seizure in the territory of the Republic of Uzbekistan, its sale and return to the requesting country have not been received.

557. As already noted, the most common way to legalize criminal proceeds is the acquisition of property (movable or immovable) by the perpetrators with its fictitious registration as property of third parties.

558. According to the established practice of LEAs, they seize the property legally registered as the property of third parties, if there is evidence of its acquisition by criminal means and its actual

ownership by a suspected or accused person. The methods of law enforcement practice have received the underlying normative consolidation at the level of statutory explanations in resolution No. 26 of the Plenum of the SC of December 27, 2016 "On the judicial practice of application of legislation for compensation for property damage caused by crime", which was supplemented on 10.06.2021 with the relevant explanations on this issue.

559. Assessors are given examples of confiscation of the property fictitiously registered as the property of third parties.

Case Study 8.10. (Confiscation of property legally owned by third parties)
In the criminal case against the head of the LLC N. it was established that he bought an apartment in Samarkand from R. for money he had gained through evasion of taxes and other obligatory payments, and in order to conceal the origin of his real rights to the property he actually possessed and used the apartment without registering it in his name.
N. was convicted by a court of committing crimes under Articles 184 (tax evasion), 189 (violation of trade rules) and 243 (ML) of the CC. The above-mentioned immovable property was forfeited to compensate for damage and for funds transfer to the state's revenue.

560. However, as the representatives of the SC explained, in some cases (as a rule, when the parties to the transaction deny its fictitiousness), for the purposes of confiscation, it is required to initiate a procedure to invalidate the transaction at the request of the prosecutor in civil proceedings, and this circumstance, according to experts, refers to aspects that complicate the application of the confiscation measure.

561. Moreover, as mentioned above, confiscation is not an institution of criminal law. Accordingly, its non-application is not an incorrect application of the criminal law, which is the basis for changing the sentence by a higher court. The non-application of confiscation is also not considered as a significant violation of the criminal procedure law. These gaps in legal regulation entail the impossibility of changing the sentence when it is reviewed by courts of higher instances (except for the cases of changing the acquittal judgement and the adoption by a higher court of a new procedural decision on the conviction of the guilty).

Case Study 8.11. (Application of confiscation when the case is reviewed by a higher court)
Yu. and A. were charged by a criminal prosecution unit with several crimes and, specifically, the crime, that they, being the directors of LLC and shadow leaders of other LLCs, acquired in the names of third parties 2 cars, houses, a restaurant for the funds gained by them through the theft of state funds obtained by larceny and embezzlement, in order to legitimize such funds by hiding their sources and real ownership rights.
In respect to the above episode, the charges of Yu. and A. were acquitted by the court of the first instance (with conviction on other elements of crimes), and it was decided to return the movable and immovable property to the legal owners. The court of appeal, at the prosecutor's protest, changed the verdict, Yu. and A. were found guilty in full of the charges, and legalized property was forfeited into compensation for damages and to the state's revenue.

562. The CPC provides for the possibility of resolving the issue of the fate of material evidence, including the confiscation of instruments of crime, at the stage of the sentence execution. However, these provisions do not apply to the recovery of the monetary equivalent of criminal proceeds from a convicted person, and therefore cannot be considered to fill in the gaps of legal regulation to a sufficient extent.

563. Examples of confiscation of property intended to be used for TF purposes are provided in the analysis of IO.9.

564. In order to increase the awareness of LEAs about the means and methods of identifying criminal assets, to improve the activity related to interim measures, educational, methodological, scientific and practical activities are being carried out in the country. The issues of confiscation of criminal assets are included in the educational and methodological plans of institutions that train and improve the skills of employees of competent departments and agencies. The state of work on ensuring the

confiscation of criminal assets was the subject of discussion at working meetings, including interdepartmental meetings, including the development and adoption of specific measures aimed at improving the effectiveness of this activity.

565. Based on the information provided, it can be seen that the competent authorities have sufficient resources (personnel, materials and technical resources, information resources) to perform their functions in the field of identifying and confiscating criminal assets.

566. Thus, assessors conclude that confiscation of proceeds, instrumentalities of crime, and property of equivalent value within the country is sufficiently effective. However, the isolated fact of confiscation of proceeds moved to other jurisdictions does not allow to conclude that criterion 8.2 is fully implemented.

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

567. In accordance with the laws of the Republic of Uzbekistan, monitoring compliance with customs legislation, prevention, detection and suppression of law violations, including smuggling, is one of the main tasks of customs authorities.

568. Control over the cross-border movement of cash and foreign currency, currency valuables is carried out by customs authorities on a comprehensive and systematic basis.

569. For these purposes, the SCC widely uses information and communication technologies, specifically, the effective functioning of an automated risk management system, automatic information systems "E-commerce" (tracking postal mail), "PTD", "GTD" (passenger and cargo customs declarations), etc., integrated with other law enforcement and government agencies, has been introduced and maintained. The SCC has also established the Situation Center, the functionality of which allows online execution of all tasks of customs authorities, including the detection and suppression of illegal cross-border movement of cash and currency valuables, operational analysis of the current situation at all customs posts of the country and prompt response to emerging threats based on a risk-based approach.

570. According to the information provided by the SCC for 2016–2020, the import of cash currency into the country exceeded the export by 1,993.1 million USD, due to the high level of labour migration of citizens of the Republic of Uzbekistan to other countries.

Table 8.5. Data on currency imports/exports in cash (in millions of USD).

No	Movement of cash currency	2016	2017	2018	2019	2020	Total
1	Import	1 709.8	2 967.8	1 993.8	2 544.4	1 419.5	10,635.3
2	Export	1 187.5	2 179.7	1 907.9	2 422.5	944.6	8 642.2
3	Difference between import and export	+522.3	+788.1	+85.9	+121.9	+474.9	+1 993.1

571. When identifying the offenses related to the illegal import and export of cash in the national currency of the Republic of Uzbekistan and foreign currency, negotiable bearer instruments, customs authorities confiscate illegally imported and exported currency, conduct pre-investigation checks, draw up administrative offense reports (Articles 227-22 of the CAO - non-declaration or false declaration of goods, as well as on other offenses) or initiate criminal proceedings (Article 182 of the CC – violation of customs legislation).

572. The customs authorities restrained the facts of illegal cross-border movements of foreign cash related both to its import into the country and export from the country.

Table 8.6. Statistics on the detection of customs offenses

Customs offenses		2016	2017	2018	2019	2020	Total
Foreign currency import (total)		301	42	32	18	9	402
including:	administrative cases	279	30	16	8	1	334
	criminal cases	22	12	16	10	8	68
Foreign currency export (total)		725	607	144	204	31	1 711
including:	administrative cases	722	602	130	186	23	1 663
	criminal cases	3	5	14	18	8	48

Total identified customs offenses		1 026	649	176	222	40	2 113
including:	administrative cases	1 001	632	146	194	24	1 997
	criminal cases	25	17	30	28	16	116

573. Thus, despite the excess of the import of foreign currency over the export in monetary terms, in most cases (81%) customs offenses were identified during the export of foreign currency, which, according to experts, indicates the need to take additional measures to ensure proper control over compliance with customs legislation when importing foreign exchange currency into the Republic of Uzbekistan, including in order to identify and restrain the facts of the possible use of cash couriers for laundering in the country of funds criminally obtained in the territory of other states, as well as the facts of TF.

574. A steady trend of decline in the number of identified customs offenses related to violation of the foreign currency declaration procedure, due to the measures for liberalization of currency policy (Decree of the President of the Republic of Uzbekistan No. UP-5177 of 02.09.2017) and, specifically, the cancellation as of 01.01.2018 of a mandatory written declaration by individuals of foreign currency for import/export in the amount equal to or not exceeding $2,000 (Decree of the President of the Republic of Uzbekistan No. UP-5276 of 06.12.2017), stating the limit value for written declaration in the amount of 70 mln UZS equivalent to 6,600 USD (Resolution No. 66 of the CM dated 30.01.2018 as amended on 10.08.2020).

Table 8.7. Information on the seizure of foreign currency and currency valuables by customs authorities (billion UZS /thou. USD at the exchange rate effective at the time of withdrawal)

No.	Withdrawal of foreign currency and currency valuables by customs authorities	2016	2017	2018	2019	2020
1	in billion UZS	2.5	3.5	7.4	15.1	2.4
2	in thousands of USD	845	680.9	917.1	1706	238.5

575. Thus, despite the decline in the number of facts of detection of customs offenses, in the period from 2016 to 2019, there was a steady increase in the amount (sums) of foreign currency seized by customs authorities, which indicates the effectiveness of the measures taken to control the cross-border movement of cash. According to the explanations of the SCC's representatives, the 2020 figures reflect a significant decrease in passenger traffic due to the measures taken by the country to stabilize the sanitary and epidemiological situation in connection with COVID-19.

576. According to the information provided by the SCC, in the period 2016–2019, 8 facts of cross-border movement of cash (USD, euros, Russian rubles, yens) in postal items were revealed. The seized currency was confiscated by the court to the state's revenue.

577. Investigation of crimes related to declaration procedure violations (Article 182 of the CC) is carried out by the investigative units of the SSS, which investigated 56 criminal cases of this category in 2016–2019, seized cash currency, including USD – 22.2 million, Russian rubles – 21.8 million, Kazakh tenge – 29.9 million.

578. Thus, the customs authorities and the SSS apply an integrated approach to identify and suppress the facts of illegal cross-border movement of cash, the seizure of currency and currency valuables is carried out on a significant scale.

579. Administrative and criminal procedure laws (Article 23 of the CAO, Articles 211, 284 of the CPC) provide for the confiscation of foreign currency as subjects of customs offense (crime) and other goods and vehicles moved in violation of the established procedure, that are tools and subjects of customs offenses (crimes).

580. According to the statistics of the SC for the period 2016–2020, 1,323 persons were convicted in 665 criminal cases for the crimes under Article 182 of the CC (violation of customs legislation). During the same period, 23,342 persons were brought to administrative responsibility under Articles 227–22 of the CAO (non-declaration or false declaration of goods).

581. The volume of confiscation by courts in the cases of customs offenses and crimes is significant.

Table 8.8. Information on the confiscation of foreign currency in the period 2016–2020 by the courts to the government

CC and CAO Articles	Confiscated foreign currency			
	US dollars	euro	Russian ruble	Other foreign currency
Article 182 of the CC	96,973,829	77,840	50,015,120	37.1 million UZS
Articles 227-22 of the CAO	226,911	5,215	46,933,114	37,1 million UZS

582. The country provides examples of the identification of customs offenses related to the violation of the procedure for cash import/export, which entailed the application of the confiscation measure.

Case study 8.12
In the customs control zone of the departure hall of the Tashkent International Airport, as a result of a body search and inspection of the hand luggage of M.W., a citizen of the People's Republic of China, who took a flight to China and went through the "green" corridor, the excessive foreign currency in the amount 7,000 USD was found, which were not presented to customs control.
By court order, citizen M.W was found guilty of committing an offense under part 1 of Article 227 22 CoAO, he was subjected to an administrative penalty in the form of a fine. The currency in the amount of 7,000 USD was confiscated to the state's revenue.

Case study 8.13
The officers of the SCC during joint operational search activities with the State Security Service in the Ferghana region detained a group of persons – citizens of Uzbekistan A. and B., who attempted to organize the illicit export of foreign currency to Kyrgyzstan outside customs control in the amount of 516,486 USD.
By the verdict of the court, A and B. were found guilty of committing a crime under Articles 25,182 part 2 of paragraph "a" and sentenced to fine and penal labour (respectively). Funds in the amount of 516,486 USD were confiscated to the state's revenue.

Case study 8.14
At the customs post on the section of the Uzbek-Tajik border at the exit to Tajikistan, the customs officers of the post carried out a customs inspection of the passenger car of a citizen of Tajikistan A., during which a currency in the total amount of 100,500 USD was revealed in the car in the stash, which was not declared and not presented for customs control.
A. was found guilty by the court of committing a crime under Article 182, part 2, paragraph "a" of the CC and was sentenced to a fine. Funds in the amount of $100,500 were confiscated to the government. The car as an instrument of crime was confiscated to the state's revenue.

583. According to the explanations contained in paragraphs 18-1 of resolution of the Plenum of the SC No. 18 dated 06.09.2013 "On the judicial practice in criminal cases of customs law violations and smuggling", vehicles used in the illicit movement of goods or other valuables across customs borders are recognized as an instrument of crime (Article 182 of the CC) when they were moved to evade or to conceal from customs control. In such a situation, vehicles are subject to confiscation in accordance with the rules of the CPC.

584. According to statistical data of the SC, 70 vehicles were confiscated in 2016–2020 as instruments of committing a crime under Article 182 of the CC.

585. Thus, the statistical data provided by the country and examples of law enforcement practice allowed assessors to conclude that in general, the confiscation of undeclared (falsely declared) cross-border movement of currency as well as instruments of customs crimes is applied in the country and is an effective, proportionate and dissuasive sanction.

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

586. According to the NRA, predicate crimes with a very high degree of risk include violation of trade rules and service provision rules; drug trafficking; corruption/bribery; tax crimes; customs crimes;

creation of a criminal community. Activity without a license is recognized as a high-risk crime. Medium-risk crimes include fraud; extortion; ecological crimes; illegal trade in medicines; illegal production of stamps, documents, and seals; and forgery. Other crimes are classified as crimes with an insignificant and low risk level of ML/TF.

587. The country has not provided information on the total number of sentences for which the confiscation measure has been applied, the amount of confiscation imposed for predicate offenses and the amount of confiscation imposed for ML criminal cases.

588. The BCE provided statistical data on the actually confiscated ML criminal proceeds according to executive documents. However, these data are not comparable with statistical data on criminal prosecution for ML crimes, broken down by predicate offenses. It is worth noted that, according to the data of the BCE, the confiscation was applied for ML criminal proceeds obtained as a result of illicit firearms trafficking, illicit trafficking of stolen and other goods, money counterfeiting. However, according to statistical data, in the period of 2016–2020, the criminal prosecution was not carried out for the ML crimes, in respect to which the above specified crimes were predicate offenses.

589. Because of the lack of reliable and comparable statistical data, it was not possible to draw conclusions about the compliance or non-compliance of the confiscation measure with the ML/TF risk assessment.

Overall conclusion on IO.8

590. The priority task of the national policy in the field of combating crime in the country is the compensation for property damage caused by crimes (restitution to victims). Confiscation of criminal proceeds is applied only if the person who suffered property damage is not identified (absent), as well as in cases when the criminally obtained property is not subject to return to the victim or exceeds the amount of damage caused by the crimes.

591. Confiscation of criminal proceeds is not an institution of criminal substantive law, is based solely on criminal procedural mechanisms and the use of non-conviction-based confiscation is limited.

592. LEAs use the granted procedural powers to identify and seize property, however, considering the peculiarities of legal regulation, their efforts were mostly focused on ensuring compensation for property damage from crimes, rather than on confiscation of criminal proceeds.

593. It should be mentioned that the compensation for property damage caused by crimes, the confiscation of criminal proceeds to a greater extent is implemented through the efforts of LEAs, but through the voluntary return of criminally acquired assets by the perpetrators seeking release from liability or significantly mitigate punishment on the basis of criminal justice rules of incentive nature.

594. Control over the cross-border movement of cash is carried out on a systematic and comprehensive basis, the confiscation of cash and instruments of customs crimes is applied, constituting an effective and dissuasive measure.

595. The country has provided various kinds of statistical data reflecting the application of confiscation. However, due to their incompleteness and incompatibility of such data, the experts could not come to final conclusions, including in terms of compliance of the confiscation results with the NRA.

596. The actual execution of court decisions in terms of confiscation of property and restitution to victims was significantly hindered in 2020 due to COVID-19. However, the decline in the effectiveness of the enforcement agencies had occurred before, the most significant one being in 2018.

597. The work on the identification and return of criminal assets moved to other countries is not sufficiently intensive.

598. **Uzbekistan is rated as having a moderate level of effectiveness for IO.8.**

CHAPTER 4. FINANCING OF TERRORISM AND PROLIFERATION FINANCING

Key findings and Recommended actions

Key findings

Immediate Outcome 9

1. The government clearly understand the threats of global terrorism and related risks. Competent authorities are well acquainted with current TF risks and adequately response to emerging challenges. Therewith, due to effective and decisive actions made by the government, the terrorist threat level in Uzbekistan has significantly decreased during the last 10 years.
2. On the whole, investigations conducted by LEAs are in line with Uzbekistan's risk profile. LEAs pay strong attention to outside TF risks, however, the risk of domestic financing seems to be underestimated to a small extent.
3. The Republic of Uzbekistan has the necessary legal framework established enabling criminal prosecution for TF. LEAs effectively and confidently co-operate with one another to identify and investigate TF cases. From 2016 to 2020, 58 persons underwent punishment for TF, all the while competent agencies never retreated from the investigation of TF cases, and all the initiated ones reached the court with only one subsequent verdict of non-guilty in respect of TF, although even in this case the person was convicted for another crime.
4. Apparently, regarding the majority of the terroristic crimes there have been conducted parallel financial investigations as well. However, the quantity of such crimes (687) detected during the 2016-2020 years shows that there are possibilities of taking a more thorough approach to the investigation of financial aspects of terroristic crimes. One more indirect proof of that: there have been no cases of terrorists' electronic assets seizure as part of relevant criminal investigations.
5. National list of terrorist organisations is related to the possibility of prosecution for TF. This state of affairs may lead to LEAs not paying attention to the financing of some international terroristic organisations (ITO), i.e. identifying and investigating FT associated with organisations, not on the national list.
6. National strategic documents settle anti-terroristic efforts as one of the country's development priorities, nevertheless, only the latest ones refer to the financing of terrorism as a separate issue.
7. In most cases of TF committed courts apply effective and proportionate sanctions. Non-custodial or probation sentences apply little, and zero recidivism convincingly demonstrates the dissuasive character of the sanctions applied.
8. Although for the last 5 years authorities have not detected any cases of legal entities' involvement in TF schemes, the only sanction envisaged for this by legislation is the possibility of legal entity liquidation. This not always can be adequate. With that, the mode of this sanction application does not assure its inevitability.
9. Competent authorities have made available different statistics regarding criminal prosecution for TF, but they seem to be largely collected manually and non-systematically.
10. The government also actively takes alternative measures when a conviction for TF proves to be a failure due to various reasons, including a conviction for other crimes and disciplinary measures.

Immediate Outcome 10

1. The Republic of Uzbekistan recently (for 2 years) had a coherent system of implementation and application of the TFS, which allows applying the TFS regime without delay. The system hadn't fully ensured the "without delay" principle in previous years.

2. The lack of cases where the Republic of Uzbekistan has submitted proposals for inclusion on the UNSC sanctions lists may be a disadvantage, given the large number of individuals on the national section of the List.

3. The mechanism of the mutual freeze of terrorist-related assets is being used: relevant enquiries are forwarded to other countries and received from there ones are considered — to take measures as to the suspension of operations and/or assets or other property freezing.
4. The procedure for amending the List and communicating it to FIs, DNFBPs and VASPs in practice takes up to 10-16 hours from the moment the grounds for doing so appear. The FIs and DNFBPs apply the TFS and implement the freezing of assets immediately after the publication of changes to the List on the website of the DCEC in the personal account. In this regard, the assessors consider that the Republic of Uzbekistan implements the TFS regime without delay.
5. There is a significant level of proportionate measures applied to vulnerable NPOs in the country, both general and targeted. Specific controls are used under the RBA, while general controls are applied within a unified regulatory and supervisory framework. Applying these measures in combination addresses the existing risk of NPOs being used for TF purposes, as evidenced by the absence of such instances in the high level of overall TF risk identified in the NRA.
6. The lack of control over the intended use of the financial assistance provided, while a weakness, is mitigated significantly by the use of non-cash settlements and the involvement of FIs in the risk mitigation processes for the use of NPOs for TF purposes.
7. Uzbekistan seeks to deprive terrorists, terrorist organisations and individuals who finance terrorist activities of their assets and the means to commit crimes through various methods, including designation, freezing of funds and confiscation as part of the investigation and prosecution of TF cases.
8. Measures having been taken by the Republic of Uzbekistan government overall correspond to the country's general TF risk profile.

Immediate Outcome 11

1. The Republic of Uzbekistan has a uniform legal framework as to proliferation and terrorism financing. In general, for 2 years the country had a coherent system of implementation and application of the TFS, which allows applying the TFS regime without delay. Despite certain legislative imperfections when it comes to implementation of the "without delay" principle, competent authorities and the private sector have made practical steps towards timely inclusion of those related to the PF into the corresponding list and informing organisations dealing with funds and other property about that and taking measures as to freezing immediately after publication on the official website of the FIU as well.
2. DCEC is a competent authority responsible for PF-related persons list drafting, maintenance and bringing it to the knowledge of supervisory bodies and reporting entities as they do in case of the TF list. The Republic of Uzbekistan can implement TFS not only pursuant to the PF UN sanction lists, but within the framework of the national regime, too, — and they can freeze assets of those related to PF in response to third-country enquiries. As of the on-site mission in June 2021, the list consisted of persons enlisted by UNSC in accord with PF Resolutions.
3. Over the reporting period there were no identifications of financial operations or other assets of persons related to PF. FIU in Uzbekistan receives and analyses PF STRs relating to Iran residents. The majority of national currency operations relates to salary and dividend payments to staff members or to founders having the Islamic Republic of Iran citizenship. The majority of foreign currency operations were carried out under export and import agreements or as visa fees or salary payments to foreign establishments, embassies and consulates staff (etc.). There also have been cases of SWIFT money transfers between individuals, however, over the 5 years, they constitute less than 2 percent of the total amount of operations. There have been no DPRK-related STR registered.
4. Some reporting entities use automated systems to secure timely access to the PF list and for the most effective execution of their TFS obligations implementation. Still, there are DNFBP sectors with not so sophisticated means of control; they check their customer bases manually.
5. Some FIs and DNFBPs face difficulties when identifying ultimate BO (client/counterparty). Therewith, supervisory bodies and FIUs clarify FIs and DNFBPs' obligations in the sphere of TFS.

6. The Republic of Uzbekistan has an effective customs and export controlling system, one of its duty being control over dual-use goods turnover (with the engagement of the MFA, SCC, State Committee on Industrial Safety (SCIF), and Ministry of Investments and Foreign Trade (MIFT) of the Republic of Uzbekistan). Moreover, the SSS conducts OIM and detective operations aimed at taking control over dual-use goods movement.
7. There is practically no trade between Uzbekistan and DPRK, while minor trade with Iran involves primarily food and consumer goods. In Uzbekistan, the Iranian capital bank keeps its operation having, however, a narrow clientele and range of activities and complying with all the AML/CFT legislative requirements.

Recommended actions

Immediate Outcome 9

1. The Republic of Uzbekistan has to keep its efforts to counter terrorism financing, including giving more accent to identifying domestic sources of TF (crowdfunding inclusive), and scrupulously conducting parallel financial investigations on TF cases, especially where there is no obvious evidence of self-financing.
2. Authorities should more often update the terroristic organisations list and ensure criminal prosecution in all cases of financing of a terroristic organisation, even if it has not been listed nationally or by UNSC but is terroristic at its core.
3. The LEAs should take further steps to put the Joint Financial Investigation Regulation[41] into practice to ensure that parallel financial investigations are conducted in all terrorism cases.
4. Currently adopted measures on the integration of TF investigations into national anti-terroristic strategies should be practically taken, and combatting of TF should be more often considered as a separate area of concern.
5. Country authorities should revise the existing approaches to the legal entities' liabilities — via creation of a mechanism ensuring the effective application of proportional restraining sanctions in cases of TF schemes involvement.
6. Competent authorities should take measures to ensure the systematic gathering of TF prosecution statistics (and their holistic character).
7. LEAs and other concerning agencies should take measures as to information policy improvement, including access to information about terrorist and extremist threats.

Immediate Outcome 10

1. The Republic of Uzbekistan should improve its efforts to propose persons to the relevant UN sanctions lists, and review the existing national section of the List to see if there are any eligible persons on it.
2. It is necessary to consider developing additional specific targeted measures for NPOs vulnerable to use for TF, including in relation to ensuring the monitoring of expenditure by public foundations and religious organisations, based on the identified threats and risks of NPOs being used for TF.
3. Increase competent authorities' engagement with NPOs and information exchange to engage NPOs in improving methods to identify and mitigate the risk of TF and related vulnerabilities and developing specific programmes to encourage NPOs to conduct transactions through regulated financial channels. Engage the donor community to participate in activities organised for NPOs.
4. Consider the possibility of granting NPOs access to the dashboard on the DCEC to enable their use of the List and timely receipt of updating notifications.

[41] This refers to the joint instruction "On the procedure for examining the financial aspects of criminal activities in the course of investigations, pre-investigations, enquiries and pre-trial investigations".

5. Ensure regular updates of NPO sectoral risk assessment, use all possible sources to identify the types of NPOs at risk of TF, define further the threats posed by terrorist entities to NPOs at risk, and how terrorists exploit community foundations and religious organisations.

Immediate Outcome 11

1. Make legislation amendments to ensure covering all natural and legal persons (in addition to FIs and DNFBPs) in terms of mandatory obligations of assets freezing within the TFS system.
2. To further improve and ensure awareness among FIs and DNFBPs regarding TFS in the proliferation sphere in order to facilitate understanding and usage of mandatory measures envisaged by sanctions applied, including with the aim of the ultimate BO identification.
3. Develop and disseminate to the private sector detailed guidance on the practical application of PF related to TFS and related typologies.
4. Consider the possibility to enhance reporting entities' abilities to identify companies owned or controlled by those enlisted — in an attempt to uncover possible PF sanction evasion.

599. This section considers and evaluates achievement of Immediate Outcomes 9-11. While effectiveness assessment, Recommendations 5-8 (as well as 1, 2, 30-32, 37, 39, and 40) have been used.

Immediate Outcome 9 (TF investigation and prosecution)

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

600. In the course of mutual evaluation, the government of the Republic of Uzbekistan have demonstrated their adherence and commitment to combating terrorism and its financing. As a result of the fruitful work of competent, legislative and judicial authorities, the level of terrorist threat in Uzbekistan has significantly reduced over the past 10 years. There have been made amendments to the Law of the Republic of Uzbekistan on Combating Terrorism and to the CC, where TF has been established as a separate article. All these have allowed authorised bodies to understand the importance of actions against not only terrorist activity itself, but against its financial backing, too. In the last 5 years[42], 58 individuals have been convicted in TF cases (see Table 9.3 for similar statistics).

601. Country authorities have assessed TF risks based on available judicial case studies and intelligence information within the NRA framework. The proximity to areas of high terrorist activity, the low incomes of the unskilled working-age population and the associated high level of labour migration to foreign countries contribute to the high level of terrorist threats.[43] These conclusions in overall correspond to estimations made by independent experts and to open data. LEAs have a clear understanding of risks. All the authorities having provided their estimations during the on-site mission have suggested almost the same information on the existing environment — that demonstrate a high-level information exchange between competent authorities of the Republic of Uzbekistan.

602. Due to decisive actions and effective coordination of law enforcements (SSS and MIA), Uzbekistan has not faced any terrorist attack for a long time already. Corresponding attempts are terminated in the course of special operations, even in difficult-to-identify cases of TF. Only during 2020, the State Security prevented four attempts of such attacks (two of them were planned in Uzbekistan, another two — within the foreign territories). In the like cases, competent authorities conduct thorough investigation and pursue those who are guilty. This is the essential moment proving the effectiveness of the authorised bodies' work, as it demonstrates their ability to confidently and without adverse consequences respond to the challenges arising.

603. The government have a good understanding of international terrorism threats and related risks, including a significant quantity of migrant workers moving to countries neighbouring to kinetic action zones. From the beginning of armed conflicts in Syria and Iraq, over 2 000 of Uzbekistan citizens

[42] From 2016 to 2020

[43] In the process of labour migration to foreign countries, Uzbek citizens are often radicalised on their territory. For more details on unemployment and labour migration, see Chapter I.

moved there for participation in armed clashes on the terrorist side. Therewith, LEAs representatives stated that they checked every such case and had all the necessary data available. Moreover, from the moment of inclusion of liability for such voyages financing into the CC (in 2016), the flow of those radically-minded significantly reduced, and such facts now are successfully being identified, investigated and stopped. Learning the national practice of TF criminal prosecution has demonstrated that many criminal cases were indeed associated with financing of such trips.

Case study 9.1. (Stopping of trip financing and export of terrorists)
From February 2014 to March 2017, person Ya was engaged in propaganda of terrorist organisation ideas via internet aiming at enlarging its range. In part, he encouraged others to Jihad and promised to help in moving to the territory of ISIL. Overall, he assisted in transferring of about 250 persons in order of their becoming new members of ITO. At the same period of time, Ya raised funds to maintain two terrorist organisations, monthly transferring USD 1-1.5 thousand to ITO members in Syria. In 2019, Ya was convicted for the financing of terrorism, mercenary activities and other crimes of terroristic nature. He was sentenced to 19 years in prison.

604. As it follows from the data presented by the Republic of Uzbekistan, up to 35 percent of identified TF cases in the country have association with domestic terrorist activity[44]. Entirely, published by media cases of armed extremist groups arresting also witness a certain level of inner terrorist activity. However, the NRA says that financing of terrorism in Uzbekistan has mainly external character. Law enforcements representatives (SSS, MIA, GPO, and DCEC) in their interviews have repeatedly underlined the minimality of the treat related to domestic TF and radicalisation of citizens mainly after their migration to other countries. This is not fully in line with the amount of convictions for terroristic crimes committed within the territory of Uzbekistan, while available examples of raising of funds for domestic terrorist groups financing say rather to the contrary (see Case studies 9.2 and 9.3).

Case study 9.2. (Becoming a member of terrorist organisation and domestic fundraising)
Starting from January 2018, person K. actively learned terrorist organisations materials available in the web, those about Jihad inclusive. Further, he entered into a terrorist organisation and from June 2018 to August 2019 had meetings with like-minded persons, Z. (‘3.’) being among them, in various places of the Tashkent region (oblast). In May 2019, K. come to an arrangement with Z. about the financing of a terrorist organisation, having raised USD 1 000. They handed the money over to Kh. (‘X’) for forwarding it to ‘Beit Al Mal’ (informal ‘money box’ of a terrorist organisation). Kh. was arrested, though, and the money he was disposed of. In 2020, K. and Z. were convicted for TF and other crimes. K. was sentenced to 11 years and 6 months of imprisonment, while Z. — to 7 years and 6 months.

605. Uzbekistan’s government are well-acquainted with various TF typologies, such as the use of zakat schemes, fundraising through ad hoc networks, the movement of funds through transfers without opening a bank account and through bank cards, the use of cash couriers, and the raising of funds through criminal activities. National FIU (DCEC) accumulates corresponding data and regularly forwards them to LEAs that, in addition, analyse and generalise the received information themselves. Meanwhile, Article 155.3 of the CC (responsibility for TF) envisages effective criminal prosecution at all stages of such financing, including the collection of funds, their transferring and use. This conclusion is proved specifically by the information on the application practice (see Core Issue 9.2) and the sentences provided by the country (some of which are described in this paper).

606. In general, LEAs suppress and effectively prosecute various types of TF, including all Central Asian specific practices such as hawala. At the same time, the nature of investigations largely corresponds to the country's risk profile, including TF from abroad through labour migrants, providing funds for travel to areas of ITO activity. Concerning domestic financing, as noted above, the LEAs effectively prevent and investigate such cases, but the level of risk involved is somewhat undervalued. Moderate improvements are needed in this area.

[44] The Republic of Uzbekistan Ministry of Internal Affairs data

TF identification and investigation

607. In Uzbekistan, pre-trials (identification (detection), suppression, solving, and investigation) of TF crimes are conducted in the form of OIA and pre-trial proceedings on criminal cases and materials. Pre-trial proceedings consist of two stages: pre-investigation check and pre-trial investigation (legal enquiry or preliminary investigation). Depending on the crime complexity, its identifying, detecting and investigation can be a combination of several forms (for example, OIA, pre-investigation check and preliminary investigation) or can be conducted solely in form of preliminary investigation that is a must in TF cases.

608. TF identifying and investigating community consists of DCEC (analytics based on STRs received), SSS and MIA (criminal intelligence and detective operations based on data from own sources, including information provided by agents, as well as on FUI analytics and information from foreign colleagues). Criminal intelligence results are forwarded to investigative authorities that issue notice of formal charge in TF against particular persons. After that, such cases go to the prosecutor's office (together with the letter of accusation) and to the court — for consideration on the merits.

Case study 9.3. (Identifying of TF cases based on FIU information)
At the beginning of 2020, the SSS received primary intelligence information from DCEC under GPO on person P.: while in Uzbekistan in 2019, he transferred to the ITO emissary Yu ('Ю.') in Turkey USD 1 200 via bank transfer. Based on the information received, SSS organised a corresponding inspection as to P. As a result, there was received confirming information about his TF engagement. SSS forwarded the materials gathered to the Investigative Department of the MIA, where in March 2020 detectives opened a criminal case against P. (CC Article 155-3). In the same year, he was convicted for terrorism financing and a range of other crimes and received 7 years of imprisonment.

Case study 9.4. (TF identifying as a result of FIU analytic activity)
At the end of 2019, DCEC received information from the banking sector regarding banking transfer by citizen A. of USD 1 200 in total to Kyrgyzstan citizen H. to Turkey. Analysis of made by A. transactions revealed TF evidence. Thus, the recipient of funds (H.) earlier was mentioned in materials of operational analysis. The information was forwarded to the SSS.
As a result of a joint SSS-MIA inspection, there was identified that A. together with four associates created a shadowy terrorist cell in Tashkent and planned to move to armed conflict zones for participation in them on the ITO side. With the aim of TF, they organised raising of funds that further were transferred to Turkey (mentioned above) and Syria.
Additionally, one of the cell members B. planned terrorist attacks (on instructions from ITO emissaries) involving religious figures killing and arrangement of explosions in entertainment facilities. These were stopped as a result of an effective special mission and house-check with gunpowder, electric detonator, potassium permanganate, aluminium powder, ammonium nitrate, etc. expropriated (purchases of all the mentioned were made at own funds).
In 2020, A. and his associates were convicted by court for terrorism financing and other felonies. All of them were sentenced to various terms of imprisonment (in particular, A. — to 11 years and B. — to 7 years).

609. Uzbekistan's LEAs have special units dealing with combating terrorism, including its financing. The country's FIU has TF-identifying units too. Here security officials noted that their approach involves considering TF, first of all, as a part of terrorist and extremist activity — therefore, CFT work is conducted by the counter-terrorism units, whose officers undergo special and advanced training in the sphere of CFT. The MIA has Main Directorate for Combating Terrorism and Extremism in its headquarters; the staff independently perform the operational activity and methodologically assist their colleagues from regional subdivisions. The same operational resources were allocated for TF combating at the SSS. In addition, both agencies have the essential detective staff.

610. To identify TF cases, LEAs use all available OIMs envisaged by the law, and composite conducting of OIMs.

611. Provided by the country statistics on pre-investigation checks of messages about TF-related crimes, opened criminal cases and investigations results allow to acknowledge that virtually in all cases competent authorities not only do not refuse to open and investigate TF-related cases but successfully lead them to accusation and forwarding to the prosecutor's office and to the court. It is important that for the entire period under review there has been neither a single refusal to open a TF criminal case nor discontinuance of such cases.

Table 9.1. *Quantity of opened[45] criminal cases on TF*

Years:		2016	2017	2018	2019	2020	Total
Criminal cases opened after TF messages check		7	14	9	11	4	45
where	MIA	4	3	4	4	2	17
	SSS	3	11	5	7	2	28

612. In accord with Article 8 of the Law on Combating Terrorism, the SSS coordinates the work of state anti-terrorist bodies, inclusive of their interaction on prevention, identification and discontinuation of terrorist activity as well as minimisation of its consequences. SSS makes a significant amount of field work on the identification of TF cases. Besides, MIA and SSS closely co-operate and effectively exchange intelligence information pursuant to corresponding inter-agency Resolution. According to common practice, when MIA autonomously identifies terrorist activity or TF patterns, SSS receives a corresponding notification. After that, the matter of further investigation is considered taking into account the power and capabilities available — for better distribution and efficiency. Practical embodiment of such approach is an important advantage of Uzbekistan's law enforcement system in combating terrorism. SSS and MIA also practice joint special operations and investigations.

Case study 9.5. (Joint MIA-SSS investigation of a TF case — via Hawala transfer system)
In 2017, person E. (Э.) with his Facebook profile came in view of law enforcements. Person A. actively communicated with E. via Facebook starting to impose religious ideas on E. in the course of their commutation. A. encouraged E. for hijrah to Syria and religious studies abroad as well as participating in ITO activity. After E.'s consent to move to Syria, A. handed him over USD 500 (via person X. dealing with illegal money transfers 'hawala') for the trip. Then E. purchased an air ticket for the Tashkent-Istanbul flight. With that, there was identified a person P. who gave E. USD 600 for the abovementioned; she communicated with A. and E. via Facebook and had been aware of the plot of the latter to move to Syria.
In the course of joint SSS-MIA operations, E. was detained while attempting to move from Uzbekistan to Turkey and then to Syria. He together with P. and X. was convicted and received long terms of imprisonment. A. was charged in absentia for the financing of terrorism and recruitment of people to take part in terrorist activity; there was put out a search for him.
The sum of 650 USD, cell phones, a laptop and data storage items were confiscated to the state revenue.

613. To make their CFT work more efficient, LEAs use various modes of interaction, including the formation of investigation teams (according to CPC Article 354) to investigate specific criminal cases of particular intricacy and importance as well as operational and tactical territorial team-ups of competent authorities' officers formed namely for combating terrorism and TF.

614. LEAs have got and effectively used the entire necessary array of tools to identify and investigate TF cases, including the possibility of intercepting communications, unofficial interviews, infiltration of agents, tracking, as well as such open investigative operations as searches and investigative interrogations (see R.31). Plus, investigators can receive practically any information needed on request (and when it involves sensitive information disclosure — subject to prosecutor's approval). During interviews, representatives of the competent authorities have demonstrated that they have and make use of the actual methodology of TF investigations that ensures usage of financial information in the process of terrorists (as well as their associates and sponsors) identification.

[45] Assessors considered the fact of TF criminal case opening as identification of such crime

615. The LEAs effectively use the available tools in the detection and pre-documentation of criminal activities related to TF.

616. Overall, competent authorities have enough power and sufficient access to electronic databases for the collection of financial intelligence in order to identify and investigate TF cases. In more detail: IO.7.

617. The GPO also has investigative divisions and can investigate TF cases when needed. However, there have not yet been such cases in GPO's practice. Prosecutors supervise the work of OIA units, in part, when it comes to their observation of criminal procedure law provisions, a regulatory regime of OIA and laws on combating terrorism. At GPO headquarters special divisions perform such supervision, while at regional prosecutor's agencies of the Republic of Uzbekistan there have been allocated corresponding staff for these duties (having consideration for the existing needs in that). Prosecutors also hear TF criminal proceedings for their forwarding to court; they argue for the state at court, too. Uzbekistan government have informed that there is no specialisation in this sphere, yet the most professional staff are entrusted to participate in such cases. In all, such an approach has proven its worth, as there was only one non-guilty verdict on the TF case over the last 5 years (see Case study 9.6).

Table 9.2. *TF criminal cases forwarded to court and guilty verdicts*

Years		2016	2017	2018	2019	2020	Total
Quantity of TF cases forwarded to court		7	14	9	11	4	45
where	MIA	4	3	4	4	2	17
	SSS	3	11	5	7	2	28

Table 9.3. TF criminal court hearings and respective sentences

Years	2016	2017	2018	2019	2020	Total
Quantity of court hearings	2	9	13	15	6	45
Quantity of persons receiving TF guilty verdicts	2	15	14	15[46]	12	58

618. As mentioned above, for the last 5 years there was one verdict of non-guilty for TF; in another case, TF subsumption was excluded from the scope of charges because the person earlier had already been convicted for committing this crime on the territory of another country. As seen from below, there have not been either grave mistakes in the process of these cases investigation or regulatory shortcomings uncovered, besides, in both cases, the guilties were convicted for other crimes of terroristic character. As a whole, TF court practice makes abundantly clear that the approaches to such crimes proving process used by law enforcements were effective.

Case study 9.6. (Verdict of non-guilty for TF)
LEA charged person H. with TF crime by transferring of RUR 1,000 (about USD 13.5 in March 2013) to an unidentified person for 'Beit Al Mal' (collective 'money box') formed by terrorist organisation members to help gunmen participating in fighting in Syria. The accusation was based solely on statements of H. given while preliminary investigation — and which he withdrew at court. In accord with CPC Article 463, the court made a decision about the failure of evidence as to H.'s commitment to TF crime and termination of criminal prosecution in respect to the abovementioned. Meanwhile, H. was found guilty of committing a crime under CC Article 244-2 (the same court decision as of May 14, 2019) and sentenced to 5 years in prison.

Case study 9.7. (Exclusion of TF from the scope of charges)
Preliminary investigation authorities charged person I. with committing crimes under CC Article 244-1 ('Manufacturing, storage and disseminating or demonstration of materials containing a threat to public order and public security') and Article 155-3 ('Financing of terrorism'). I. was found guilty (court

[46] In 2019, a person was declared not guilty in respect of TF, while in case of another person TF subsumption was excluded from the scope of charges

decision as of September 11, 2019) of committing a crime under CC Article 244-1. It was also identified that earlier he was sentenced by the Russian Federation court to 4 years in prison for the financing of terrorism. According to CC Article 8, no one could be tried twice for the same crime. In the circumstances, subsumption under Article 155-3 'Financing of terrorism' was excluded from the scope of charges.

619. The SSS has internal instruction in place as to financial investigations (classified). Moreover, in May 2021, law enforcement agencies (GPO, SSS, MIA, and DCEC) adopted common instruction 'On the procedure for analysis of financial aspects of criminal activity under criminal intelligence and detective operations, pre-investigation review, legal enquiry, and preliminary investigation' regulating parallel financial investigations of TF cases in detail. Prosecutors oversee compliance with the requirements of this document. However, despite such a recent adoption of the abovementioned instruction, investigative practice as to TF cases shows that law enforcement agencies earlier have also conducted parallel financial investigations in cases of terroristic crimes, duly examining their financial aspect. Generally, the majority of TF crimes went with terroristic crimes investigations, accumulative sentencing having been applied. Therewith, when it came to internal terrorism, there often was expressed an opinion of LEA about self-financing cases.

Case study 9.8. (Identifying of TF cases in the course of terrorist activity investigations)
During 2019-2020, SSS together with MIA conducted criminal intelligence and detective activities on the termination of functioning of the criminal extremist gang in Tashkent consisting of international terrorist organisation followers. On the basis of information gathered by field units, MIA Investigative Department opened a criminal case under CC Article 244-2 'Formation, directing and participation in extremist religious, separatist, fundamentalist and other prohibited organisations'. By further operative investigative activities, there was identified the fact of handing over of USD 1 000 (for covering travel expenses) by gang leader A. to another member Sh. ('Ш.') who planned to move to Syria. Due to measures taken, money was partially expropriated at the Sh. residential address and confiscated to the state revenue.
After investigation A. was accused of committing a range of crimes, financing of terrorism inclusive. He was found guilty by the court and received 11.5 [years] in prison. Sh. was also found guilty and sentenced to 7 years of imprisonment.

620. The sensitive character of the counter-terrorist activity issues does not allow to review every criminal case of terrorism-related nature opening and investigating as to conducting of a parallel financial investigation. However, comparing quantities of terror- and TF-related criminal cases can show that the aspect of financing has not been examined in all without any exception cases. In support of this: in the criminal procedure legislation there are no requirements as to the mentioned (CPC Article 82).

Table 9.4. Quantity of terrorism- and TF-related crimes identified

Years	2016	2017	2018	2019	2020	Total
Terrorism-related criminal cases (opened)	201	201	86	103	96	687
TF-related cases (opened)	7	14	9	11	4	45

621. Alongside with certain signs of somewhat restricted practice of parallel financial investigations use (see above), zero cases of terrorist's VA seizure during the investigation of criminal cases is a source of concern. In their explanation of this, representatives of competent authorities have mentioned that nationally TF activity mainly involves cash, while electronic payments are not frequent. Nonetheless, the law enforcement practice studied says to the contrary: for raising funds the Uzbek financial organisations' banking cards were used among other means (see Case study 9.11) and monies were transferred via a bank (see Case study 9.3)

622. Competent authorities of the Republic of Uzbekistan actively exchange information with their foreign colleagues. This is particularly important bearing in mind the role of foreign component in the Uzbekistan TF risks system. Such the exchange is performed based on intergovernmental memoranda and agreements, as well as via international and regional LEA networks (see IO.2).

Steadiness and effectiveness of the contacts are confirmed by the specific practical outcomes under the TF profile.

Case study 9.9 (Identifying TF cases together with foreign colleagues)
SSS performed criminal intelligence analyses regarding person A. who returned to the Republic of Uzbekistan after working abroad where he had been recruited by ITO emissaries. It was identified that after his return home, A. created a jihadist cell and a Telegram channel, allegedly for raising funds for the reconstruction of temples suffered from the breakdown of Sardoba water reservoir. In reality, he planned to hand collected money over for TF purposes. A. gave the data of 'X-bank' banking card for making money transfers; monies received he transferred to the 'C-bank' card to his relative, person B. (he worked then in Russian Federation) who readdressed the funds to ITO members in Syria. Moreover, A. agitationally convinced Uzbek citizen G. who also then worked in Russia to financially support an international terrorist organisation. Later G. transferred for TF purposes RUR 11,000 (USD 150).
To obtain evidence of A.'s engagement in the said crimes, the corresponding findings were forwarded to the FSB of Russia. While working over the findings, Russian colleagues have made interrogatory arrangements allowing to receive confessionary evidence from B. and G. The legalised materials were handed over via MIA of Russia to the MIA of Uzbekistan. Detectives of the latter filed a corresponding charge in TF; the related criminal case was submitted to the court.

623. According to law, criminal prosecution for the financing of a terrorist organisation is possible only if it is either recognised as such in Uzbekistan or included in the UN list (see R.5). In their interviews, law enforcement and judiciary representatives have explained that if receiving finance terrorist organisation is not nationally or UN enlisted, criminal prosecution is possible only through the accusation of complicity. Even disregarding the technical compliance aspect, active labour migration to other countries should be taken into account. In the circumstances, such an approach can lead to a good number's of TF cases escaping the attention of LEAs: when there are no links to financing of a specific fighter or terrorist attack and when the organisation is not included in corresponding lists. It can be so even if citizens are involved in such schemes, as there is no direct responsibility for that.

624. The situation looks more serious in the light of the fact that the national terrorist organisation list was not updated after its adoption by the Supreme Court in 2016. The government assures that all the terrorist organisations functioning in the Republic of Uzbekistan have been enlisted. This appears to be highly unlikely because since establishing of such a list in all neighbouring states (Russia, Kyrgyzstan, Tajikistan, Kazakhstan), the national lists have been updated — but that is not the case in Uzbekistan. Besides, the mass media reported Uzbek citizens' participation in terrorist organisations not recognised as such in Uzbekistan (for example, 'Guide to ISIL'). This information highlights the need for great efforts of the competent authorities regarding the actualisation of the list, providing its relation to the possibility of criminal prosecution for TO financing.

625. During the on-site mission, the LEAs provided various statistics on the identification, investigation and discontinuation of TF, however, it looks like those data were in part collected manually and this aspect earlier received less attention comparing with the time of evaluation process. It has indirect confirmation by the fact that there is a difference between the quantity of TF court sentences communicated to the assessors and that indicated in NRA[47]. Statistics provided by the state bodies (MIA, SSS, and GPO) were also of fractional character. Moreover, despite occasional consideration of practical aspects of TF crimes identification, investigation and discontinuation in various informational and guiding materials, as seen, substantive generalisation of judicial and investigative practice in this respect was not carried out. All this environment highlights the necessity to improve the terror- and TF-related cases statistical observation quality both criminologically and for the purpose of the effectiveness of competent authorities' work assessment.

626. The Republic of Uzbekistan has an extensive learning and teaching base ensuring advanced training of staff dealing with counter-terrorism and TF issues. The relevant training is performed at the GPO,

[47] According to NRA, during 2016-2018 there were 14 court sentences, while the evaluation mission was provided with the information about 24 sentences for the same period (based on the Supreme Court data)

MIA and SSS Academies, in addition, law enforcement officers take part in educational programmes of the International Training and Methodology Centre for Financial Monitoring (ITMCFM, Moscow) and other CFT training. In particular, annually several thousand of AML/CFT system of the Republic of Uzbekistan staff have GPO Academy-based advanced training, including specialised courses on 'Introduction to the investigation of TF-related crimes' and 'Training of national instructors in the sphere of combating the financing of terrorism (CFT)'.

627. Thus, the Uzbek authorities effectively detect and investigate TF cases, both as part of ongoing parallel financial investigations and as stand-alone cases, identifying them based on criminal intelligence.

TF investigation integrated with –and supportive of- national strategies

628. Combating terrorism issues have been implemented into the majority of strategical documents of the Republic of Uzbekistan, some of them being confidential and thus cannot be presented here in detail. Nevertheless, the assessors are certain that they have been hosted at the highest level. Therewith, the government have not limited themselves to considering combating terrorism issues only from the perspective of law enforcement — they have also established enhancing of work in this field as national development priority. In particular, the Strategy on Five Development Priorities of the Republic of Uzbekistan for 2017-2021 adopted by the President of the Republic of Uzbekistan Decree No. UP-4947 (УП-4947) as of February 7, 2017, provides for strengthening organisational and practical measures to prevent religious extremism and terrorism. This approach demonstrates due attention to counterterrorism efforts, their priority status being out of the question.

629. With that, until recently, combating the financing of terrorism issues has had a limited reflection in strategic documents. In the key Law on Combating Terrorism TF has been mentioned just episodically. Thus, in the context of issues that are before the state bodies engaged in combating terrorism, the powers relating to TF are identified only with respect to DCEC. The system-forming law 'On Combating Illegal Proceeds Legalisation, Financing of Terrorism and Proliferation Financing' also says about CFT measures solely from the perspective of FIU competence and financial measures — not mentioning, though, the need to counter this from the point of law enforcements' powers. It should be noted that the said laws contain different definitions of financing of terrorism that even if do not produce direct regulatory conflict do have clearly unlike scope.

630. The National Security Strategy is a closed document (the assessors have been made aware of it), but it deals with combating TF as part of a set of measures to counter terrorism.

631. In the course of the on-site mission, law enforcement representatives have generally confirmed assumptions about CFT issues being almost always (or at least predominantly) considered in the context of the anti-terrorist activity, as accompanying but not independent ones. This outcome has its confirmation by the following: within the framework of coordination activity TF issues have hardly ever been analysed as those independent (just as an element of anti-terrorist work) — despite the obligation imposed on the prosecution bodies by the General Prosecutor of the Republic of Uzbekistan order No. 129 as of February 22, 2016, to analyse CFT outcomes of the law enforcements no less frequently than once a year.

632. It should be said that lately situation with more substantive consideration of TF issues has begun to change. Thus, in May 2021 the meeting of the Coordination Council of the Law Enforcement Agencies took place, where there were discussed aspects of AML/CFT activity, particular attention having been paid to TF-related issues and to the measures of their overcoming. Among other moments, there has been pointed to the need to examine the financial aspect of criminal activity in the course of criminal intelligence and detective activities and preliminary investigation as well.

633. One more important step on the way of CFT priorities promotion in Uzbekistan's strategic documents is the adoption of the country's National Strategy on Combating Extremism and Terrorism for 2021–2026 years. Although we have yet to wait for practical implementation of its outcomes (as the document was approved by the President of the Republic of Uzbekistan only on July 1, 2021), the

fact of the CFT agenda being its leitmotif is an absolute plus. It is thus obvious that the country is on the right way, however, it has yet not been gone through, and further efforts are required to make the process complete.

634. Coordination of anti-terrorist activity, including law enforcement aspects of TF combating, is carried out through various interagency formats, a part of which is being confidential because of the specific nature of this sphere. Strategic coordination is performed by the Interagency Commission on Combating Illegal Proceeds Legalisation, Financing of Terrorism and Proliferation Financing. Still, it looks like its powers are more of general nature, not about the law enforcement aspects of CFT.

635. LEAs (MIA, CCC) have operational plans in place, where anti-terrorism and anti-extremism issues are from time to time embodied; the plans are confidential, though. Corresponding moments are also considered at the panels held by the bodies mentioned.

636. The Republic of Uzbekistan participates in the possible majority of regional and international coordinative formats relating to combating terrorism, including CIS ATC, SCO RATS, C5+1, TURKKON, etc.

637. Despite the perceived shortage of national coordinative platforms, overall competent authorities manage to effectively interact and distribute the resources available well. It is proved by both the abovementioned statistics on TF investigation and prosecution and by zero terrorist attacks in the country notwithstanding the existing geographical risks and occurrence of such crimes in the neighbouring countries.

638. The authorities of the Republic of Uzbekistan have integrated TF issues to a greater extent into national counter-terrorism strategies. They are conducting TF investigations in support of counter-terrorism policies and investigations.

Effectiveness, proportionality and dissuasiveness of sanctions

639. CC Article 155.3 envisages the following criminal liability for TF: from 8 to 10 years of imprisonment, and in case of crime repetition or committing it by an official, dangerous recidivist or organised gang the penalty can be from 10 to 15 years. There are no alternative penalty measures envisaged by law.

640. While applying sanctions envisaged by CC Article 155.3 towards those convicted for TF, courts approach the issue of penalty imposing strictly enough. Almost all the persons judged have received various terms of imprisonment; only in 7 percent[48] of cases courts have imposed restriction of freedom[49], and one case has involved a conditional sentence.

Table 9.5. Imprisonment as a sentence for TF[50]

Years	2016	2017	2018	2019	2020	Total
from 3 to 4 years			1		2	
from 5 to 7 years		1	2	6[51]	3	
from 8 to 9 years	1	2	9	3	3	1
from 10 to 15 years	1	12	1	2	2	1
16 years and more			1	2		

641. As seen from the table above, in about a quarter of cases courts have applied provisions of the CC Article 57 and have imposed the penalty that is lower than envisaged by the CC Article 155-3, even despite the fact that almost all the verdicts have been determined by cumulation of several crimes of terrorist nature. One case implied a conditional sentence. In their explanations of such an approach, representatives of the judicial system mentioned that in each case the penalty was determined with

[48] Overall, there were 5 cases of imprisonment out of 60 TF sentences (3 cases in 2019 and 2 — in 2020)
[49] Under Article 48[1] of the CC, the restriction of freedom consists of a court order prohibiting persons from leaving their home altogether or restricting them to leave their home at certain times of the day.
[50] Statistics provided are based on the information from TF verdicts provided by the country
[51] One of the sentenced to imprisonment has received a conditional sentence

consideration of the person's degree of culpability and reformation possibilities. While making an analysis of this approach, two moments should be taken into account: 1) due to grave enough TF sanctions in the Republic of Uzbekistan compared to other Global Network member states penalty decisions on the whole do not look too lenient; 2) practically zero recidivism pointed at by representatives of law enforcements during their interviews confirms the achievement of penalty goals as a result of sanctions applied to the extent they are imposed by courts now. The country has also handed over to the assessors backgrounds on the majority of cases where CC Article 57 provisions were applied. Their analysis demonstrates that while elaborating a specific decision as to sanctions, courts are really guided by the actual circumstances (low significance of deeds appearing among others) requiring imposing more lenient penalty.

Case study 9.10. (Sentencing under CC Article 57 to imprisonment for the lower than envisaged by the CC Article 155-3 term)
In April 2018, an Uzbekistan citizen I. (И.) while being in the Russian Federation as a labour migrant, appeared to be exposed to the negative influence of ITO members. To support fighters in Syria, he via the internet forwarded RUR 200 (about USD 2.5) through the payment system to the account he was provided to during correspondence in messenger. He was found guilty of TF, extremist materials keeping and participation in prohibited organisation activity by court decision as of September 18, 2019, under CC Article 57, having received 5 years in prison.

Case study 9.11. (Sentencing under CC Article 57 to the restriction of freedom)
In February 2019, person A. created a profile on a popular social network and used it to look through a video encouraging Jihad. From a virtual correspondence with another user of the same social network, he leant about the latter's current Jihad. Under the influence of his conversant summons, A. decided to forward the money to support international terrorist organisation members. After that, he transferred USD 200 via 'X-bank' in Danau to the Moscow account provided to him. He was found guilty of crimes envisaged by CC Article 155-3 and Article 244-1 (court decision as of November 9, 2020) with provisions of the CC Article 57 having been applied; A. received 4 years of restriction of freedom.

642. Comparing sanctions imposed by courts for TF with those for other crimes of terrorist nature, one should bear in mind that, as a rule, there are cases of cumulative responsibility as on such crimes, while the penalty is a sum of envisaged punitive measures, entirely or partially (CC Article 59). All in all, a person serves the resulting sentence for the entire proven terrorist activity, including TF — that makes separate weighing of a TF part in the final verdict hardly reasonable. However, for the last 5 years, there was one court verdict in Uzbekistan with financing of the terrorism as the only crime incriminated. In this case, sanctions applied can also be described as sufficient and restraining.

Case study 9.12. (Sentence for TF without cumulative charges applied)
In May 2019, person A. handed over USD 100 to person U. for his move to Syria for Jihad. Then, in June 2019, person M. handed over 400 000 UZS (about USD 40) to the same person for the same purpose. A. and M. were found guilty of the crime envisaged by CC Article 155-3 by court decision as of November 18, 2019, with provisions of the CC Article 57 having been applied; they received 4 years of the restriction of freedom each.

643. In the course of the on-site mission, Uzbekistan authorities informed that for the last 5 years they did not register any cases of terrorist crime repetition[52], TF cases inclusive. Such a result indisputably acknowledges the effectiveness of the terroristic crimes recidivism prevention system working in the country.

644. In the Republic of Uzbekistan, there is virtually no legal entity liability framework for cases when an individual responsible for the legal entity management or supervision is involved in the financing of terrorism. The only measure is the liquidation of the legal entity on grounds of its involvement in activity forbidden by law (Article 53 of the Civil Code). It should be mentioned that over the last 5

[52] This information relates only to internal terrorist activity and not to participation of the country's citizens in military conflicts on the terrotist side within the territories of foreign countries

years this measure was not applied, and the application of the like sanctions to legal entities of complex structure would hardly be appropriate. During the on-site mission, the government pointed at zero cases having been identified for the participation of legal entities in criminal schemes lately. This statement is difficult to check provided the latent nature of the criminal activity, though, the court practice considered does not make it possible to disprove it. Nonetheless, one of the possible grounds of such zero TF-involvement of legal entities can be law enforcements' lacking of target reference points for identifying corresponding cases due to zero law liability of legal entities — but not because of their actual absence. Moreover, the mechanism of the legal entities' prosecution does not permit ensuring compliance with the principle of punishment inevitability and to specify which body should be responsible for identifying such facts, gathering of materials and their forwarding to court.

645. The Uzbekistani authorities are very much in favour of applying proportionate and dissuasive sanctions to individuals, and the country requires only minor improvements for such cases. However, a system of liability rules for legal persons involved in criminal activity is virtually non-existent. This situation is somewhat counterbalanced by the liability of company managers and other employees whose involvement in TF schemes is potential. Nevertheless, moderate improvements are needed in this part of the country.

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

646. As a rule, in cases of TF, the authorities resort to criminal prosecution for the corresponding crimes or another offence of terrorist character when it is impossible to prove the very fact of terrorism financing. Law enforcement representatives pointed out that they always consider the possibility to identify patterns of another crime in the person's deeds when it is impossible to have a TF charge for any reason. Noteworthy, that within the scope of legal prosecution practice studied there was the only case of non-guilty verdict for TF. In this case, the person was convicted for other crimes of terroristic nature (see Case study 9.6).

647. The government of Uzbekistan are strongly focused on crime prevention moments, including terroristic crimes and their financing. Article 5 of the specialised Law on Combating Terrorism is dedicated to terrorism prevention. The Article underlines the need to adopt a set of political, social, economic, legal and other preventative measures not only by state bodies but by self-governments and public associations as well. Measures on crime prevention are fully regulated by the Law on Prevention of Offences, according to which the country's Cabinet of Ministers, law enforcement and self-government bodies as well as non-profit organisations are involved in this work. The Cabinet of Ministers together with MIA elaborate the state programme of crime prevention; competent authorities have the corresponding document at their disposal. The National Interagency Commission on Prevention of Offences and Combating Crime, acting upon the said specialised law and the President of the Republic of Uzbekistan Resolution as of March 14, 2017, No. PP-2833 (ПП-2833), coordinates the authority agencies' offence preventative work.

648. To prevent extremist and terrorist trends among youth, the Republic of Uzbekistan employs a unified national policy aimed at this age group. The need to protect the youth from terrorist, religious extremist, separatist, and fundamentalist ideas has been accentuated in Article 5 of the Law of the National Youth Policy. The respective national programme is also in place; prosecutory and internal affairs authorities participate, among others, in its realisation.

649. Internal affairs bodies keep track of persons having committed crimes and preventatively register those with criminal records and those having their criminal prosecution terminated on reasons other than exoneration. SSS keeps records of persons prone to offences violating peace and safety. The national government adhere to a unified approach employing a universal, specialised and individual prevention strategy.

650. As has been mentioned above, more than 2 000 of the Republic of Uzbekistan citizens have moved to high terrorist activity zones. State authorities monitor the situation and, as a result, special services

have launched at once several operations aimed at repatriation of Uzbekistan citizens who refused from extreme ideas and decided to stop their cooperation with ISIL, as well as women and children who moved to hot zones following their relatives.

651. According to Article 5 of the Law on Combating Terrorism, foreign citizens and stateless persons related to terrorist activity are prohibited from the entrance to the Republic of Uzbekistan. The relevant decision is taken in accordance with the procedure and on the grounds set out in article 29 of the Legal Status of Foreign Nationals and Stateless Persons Law. While crossing the state border, competent authorities perform passport checking. Towards people entering the country preventative and awareness-raising work is performed.

652. In the course of the on-site mission, SSS and MIA representatives demonstrated measures taken to produce and distribute media materials targeted at de-radicalising the population and ideological combating extremism and terrorism.

653. The country's competent authorities also take extensive de-radicalization and prevention measures in prisons. This work is carried out by the Central Penal Correction Department of the Ministry of Internal Affairs in cooperation with the Directorate-General for Combating Terrorism and Extremism. The forces and means employed are sufficient and the methods used are effective.

654. The Republic of Uzbekistan effectively takes alternative measures where conviction is not possible, these efforts achieve the desired result to a very large extent, so minor improvements are required.

Overall conclusions on IO.9

655. The Republic of Uzbekistan faces serious TF threats. At the same time, the authorities are well aware of the risk profile, including risks associated with international terrorism and the country's context. However, the threats related to domestic TF are underestimated to a small extent.

656. The Republic of Uzbekistan has an adequate legal framework to identify, investigate, and prosecute TF cases effectively. LEA staff are highly qualified and well-resourced and conduct effective operations against TF. The competent authorities prosecute about 10 TF cases every year, and in virtually all of the cases, they have successfully secured convictions. Over the past five years, 58 persons have been convicted of TF.

657. Those convicted are subject to severe dissuasive sanctions, primarily custodial. Legal entities are not subject to TF prosecution; however, their involvement in TF schemes is not typical for the country.

658. Uzbekistan's counter-terrorism strategies include CFT, and the LEAs broadly conduct parallel financial investigations to support them. However, such investigations do not cover all potential cases where TF could occur.

659. The country applies alternative measures effectively and efficiently in all situations where it is impossible to obtain a conviction for TF. The prevalence of such measures is vast and covers all high-risk areas. Combining these circumstances indicates that the result is primarily achieved, and minor improvement is needed.

660. **The Republic of Uzbekistan is rated as having a substantial level of effectiveness for IO.9.**

Immediate Outcome 10 (TF preventative measures and financial sanctions)

661. In the respective part of the report on the Republic of Uzbekistan legislation technical compliance to the provisions of the Recommendation 6 there has been noted incomplete arrangements for the immediacy of TFS application principle in regulatory legal instruments.

662. However, in practice, the Republic of Uzbekistan has made significant efforts to secure their timely and prompt application.

Implementation of targeted financial sanctions for TF without delay

663. Lately, a largely effective system of implementing TFS under UNSCRs 1267 and 1373 acts in Uzbekistan, which the country demonstrated to the assessors during the on-site mission.

664. There have been no cases of propositions from the Republic of Uzbekistan to expand the UNSC sanction lists. At the same time, given that there are 1,837 individuals on the national section of the List in Uzbekistan, it is conceivable that individuals who meet the criteria for inclusion on the UNSC sanctions lists could be.

665. The FIU includes the designated persons into the List in a timely manner (by 16 hours) and communicates it to the supervisory authorities, FIs, DNFBPs and VASPs. In turn, the reporting entities immediately after the publication of the List in their personal account on the website of the DCEC apply the TFS and freeze the available assets.

666. The assessors had the opportunity to familiarise themselves with the mechanism of updating the List and communicating it, including methods of updating the information, response to possible technical failures, etc., which resulted in the conclusion that the mechanism works, information is communicated without delay to competent authorities and reporting entities, despite existing deficiencies in the legislation, measures to apply the TFS are taken without delay.

667. The List amendment,communicating it to FIs, DNFBPs and VASPs and freezing procedure takes in practice up to 10-16 hours from corresponding grounds arising. That is why assessors consider that the Republic of Uzbekistan implements the TFS within 24 hours, i.e. without delay[53].

668. Relying on the data showcased, assessors come to the conclusion that such a coherent system of TFS implementation and application functions for the last two years. In the earlier period, experts believe that the system operated within the time frame described in the TC, i.e. it did not fully enforce the "without delay" principle.

669. As of the time of the on-site mission, the List consisted of 3 292 entries, including individuals and organisations relating to Al-Qaeda, Taliban movement, ITO Islamic State (ISIL) as well as to those whether directly or indirectly involved in terrorist activity according to UNSC Resolutions No. 1267 (1999), 1989 (2011), 1988 (2011), 1718 (2006), 2140 (2014), 2253 (2015), 1518 (2003), 751 (1992), 1907 (2009), 1970 (2011), and 2206 (2015) as well as to other succeeding resolutions.

Table 10.1. Information on including to the List

	Individuals	Legal entities	Total
UNSC sanction lists	396	94	490
Foreign states enquires	965		965
National list	1 815	22	1 837
Total			3 292

Formation and updating of the List without delay

670. As a law enforcement body, DCEC has a system of 24-hour duty. It presupposes authorised officers' daily monitoring of UNSC press releases and amendments to the lists published on the UNSC website. The staff number of the division responsible for the List keeping (the data were provided to assessors) enables routine monitoring within designated time intervals.

671. In case of discrepancy identification, an authorised officer immediately prepares corresponding amendments to the list and agrees on them with the executive officer.

672. Within 3 hours, the updated list is communicated to competent state and supervisory bodies and reporting entities by means as follows:

- Forwarding to supervisory bodies via the electronic channel of communication
- Forwarding to the CB and Banks via electronic channel of communication

[53] Following the on-site mission, the assessed country adopted amendments to the NLA regulating the procedure for the implementation and application of the TFS, which eliminated the deficiencies noted in Recommendations 6 and 7 regarding compliance with the "without delay" principle of applying the TFS (Order of the Prosecutor General of 30.07.2021 No. 53-B on approval of the new edition of the Regulation on the procedure for suspending transactions, freezing cash or other property, providing access to frozen property and resuming transactions of persons included in the TFS.

- Publishing on the open part of the DCEC website
- Publishing in reporting entities' accounts at the DCEC website
- Placement of news on the DCEC website
- Informational message in DCEC Telegram channel.

673. Assessors analysed the duration of the amendments to the List and its communication to the reporting entities. As a result, it was found that in all cases, the time for updating the List and communicating it to the reporting entities did not exceed one day. It should be taken into account that the time difference between Tashkent and New York is 9 hours, i.e. if a person is added to the UN sanctions list at the end of the working day in Tashkent it is already the next day at that time.

Table 10.2. Analysis of the time taken to update the List

Date of change in the UNSC list	UNSC decision	Publication on the website of the DCEC	Number of days to publish
22.04.2019	Excluded 1 item	23.04.2019	<1
01.05.2019	Added 1 item Added changes to the 80 items	02.05.2019	<1
14.05.2019	Added 1 item Excluded 1 item	15.05.2019	<1
21.05.2019	Excluded 1 item	22.05.2019	<1
09.08.2019	Changed 1 item	10.08.2019	<1
14.08.2019	Added 2 items	15.08.2019	<1
20.08.2019	Changed 1 item	21.08.2019	<1
11.10.2019	Changed 1 item	12.10.2019	<1
05.11.2019	Excluded 1 item	06.11.2019	<1
14.01.2020	Changed 85 items	15.01.2020	<1
04.02.2020	Added 1 item	05.02.2020	<1
18.02.2020	Excluded 2 items	19.02.2020	<1
23.02.2020	Added 2 items	24.02.2020	<1
04.03.2020	Added 3 items	05.03.2020	<1
24.03.2020	Excluded 1 item	25.03.2020	<1
21.05.2020	Added 1 item	22.05.2020	<1
16.07.2020	Added 1 item	17.07.2020	<1
10.09.2020	Changed 11 items	11.09.2020	<1
08.10.2020	Added 1 item	09.10.2020	<1
19.02.2021	Excluded 2 items	20.02.2021	<1
23.02.2021	Changed 92 items	24.02.2021	<1
23.03.2021	Changed 8 items	24.03.2021	<1
06.04.2021	Changed 1 item	07.04.2021	<1
17.06.2021	Added 1 item	18.06.2021	<1

674. Assessors were provided with the considerable number of relevant documents, printings, scans, activity time detailing materials, etc., — which confirms the facts of the inclusion without delay in the sections of the List of persons involved in terrorist activities.

Case study 10.1

On April 6, 2021 UNSC published on the website notification about the list entry amendments relating Abu Bakar Baasyir.

The List was updated no later than 9:45 April 7, 2021.

According to message sending data, notification about List updating was sent to supervisory bodies via electronic channel at 9:45 and it was read by all bodies no later than 11:30 same day.

The updated List was sent via electronic channel of communication to the Central Bank and to commercial banks at 9:41. At the same time the updated List and corresponding notification were published on the DCEC website. A message in Telegram was published at 10:00. At the same time, the software product of the FIs downloads the updated List from the website of the DCEC and checks the data of the client base. If there is a match, the assets are frozen.

675. The MFA also informs DCEC and competent authorities of the Republic of Uzbekistan about sanction lists comprised by UN Security Council Committees and corresponding UNSCRs once available

through official channels. This is, in essence, an additional means of control over the completeness of the List amendments actually made already in the course of daily monitoring.

676. Including persons into the List based on foreign competent authorities' enquiries is made up of two stages: considering compliance with the enlisting criteria in accord with UNSC Resolutions and making a decision regarding enlisting or refusal. Statistics on persons enlisted based on such enquiries are provided in the table below.

Table 10.3. Statistics on including of persons into the List based on foreign competent authorities' enquiries

Year	Country	Quantity of persons in enquiry	Quantity of persons enlisted	Quantity of non-enlisted
2017	Russia	419	419	0
2020	Russia	586	457	129
2021	Kazakhstan	86	86	0
	Kyrgyzstan	3	3	0

677. The mechanism of the mutual freeze of terrorist-related assets is being used: relevant enquiries are forwarded to other countries and received from there ones are considered — to take measures as to the suspension of operations and/or assets or other property freezing. For example, in 2017 there was carried out an exchange of lists of persons involved in terrorist activity; as a result, 419 persons submitted by the RF side were included in the Republic of Uzbekistan list.

678. Non-compliance with the inclusion requirements consists grounds for refusal to include a person into the List for the mutual freeze of assets. It can also be determined by different approaches adopted by countries for keeping the list[54]. Of the 129 individuals who were rejected for inclusion on the List, 14 were involved in extremist activities (only individuals involved in terrorist activities are included), and 115 were already on the List.

Table 10.4. Information on enquiries of the Republic of Uzbekistan FIU to foreign states regarding freezing of assets belonging to persons involved into terrorist activity

Year	Country	Quantity of persons
2018	Russia	26
2019	Kazakhstan	65
2020	Russia	50

679. Inclusion into the List and its communicating to the reporting entities based on the enquiries of foreign competent bodies do not exceed 24 hours from the receiving of request.

Case study 10.2

On June 21, 2021 DCEC received the foreign competent body enquiry on enlisting of three individuals. The List was updated on June 21, 2021 no later than 12:00.

According to message sending data, notification about List updating was sent to supervisory bodies via electronic channel at 17:03, while to the Central Bank and to commercial banks — at 16:59.

At the same time the updated List and corresponding notification were published on the DCEC website. In accounts on the website the updated list appeared at 12:03. A message in Telegram was published at 17:15. At the same time, the software product of the FIs downloads the updated List from the website of the DCEC and checks the data of the client base. If there is a match, the assets are frozen.

680. Requests of the Uzbekistan competent authorities on inclusion into the national List are considered in a similar way.

Table 10.5. Enquiries of the Uzbekistan competent authorities on inclusion into the national List

Year	Persons included	Persons excluded
2017	45	

[54] In Uzbekistan, only those involved into terrorist activity are enlisted, while in Russia, for example, the List includes extremism-related persons as well

2018	90	
2019		
2020	354	5
2021	1 353	

681. With that, competent authorities representatives said that, as a rule, the documents to be forwarded to DCEC for enlisting are prepared beforehand, simultaneously with the preparation of the documents envisaged by clause 6 of the Provision within the General Prosecutor's order as of September 30, 2016 No. 22-B, providing grounds for inclusion into the List. Thus the period between arising of grounds for enlisting and documents' reaching the DCEC becomes minimal.

682. For example, according to the established procedure and subject to the intra-MIA order, alongside with the case opening or filing accusation the information for inclusion in the list is immediately sent to DCEC. Data are provided in .pdf and then simultaneously forwarded via specialised mail. From MIA territorial subdivisions the data are forwarded to DCEC via MIA central office. At this, before making a decision that is the reason for enlisting, information should be agreed upon with SSS. When such, SSS also communicates with DCEC notifying them that MIA is sending information for enlisting. Whereas all the bodies mentioned are the law enforcement ones and carry out their duties at the weekend, too, operating procedures then are the same.

683. To SSS, the data for national enlisting are also forwarded on weekdays and weekends, as well as in the evening. On average, sending documents and inclusion in the List take up to 24 hours. Despite the fact that Provision within the General Prosecutor's order as of September 30, 2016 No. 22-B presupposes a timeframe up to 72 hours, the intra-SSS regulation requests to perform this within 24 hours.

684. It should also be mentioned that as most often enlisting on the grounds of MIA and SSS enquiries is performed as a consequence of the corresponding criminal cases investigation, the need to prepare documents for their forwarding to DCEC would not be something unexpected for a detective. The entire set of documentation is prepared simultaneously with documents on making a decision that is the reason for enlisting (opening of a criminal case, indictment order, etc.). In urgent cases, a detective is empowered to forward material directly to DCEC at his own discretion.

685. The relevant documents are sent electronically and later if needed, a hard copy is forwarded. Control over this process is carried out by the head of the corresponding division. When a document is sent via electronic channels, its hard copy is stamped accordingly.

686. SSS also controls outcomes of enlisting documents consideration. For the full and timely application of TFS, a detective identifies the assists of the person to be enlisted simultaneously with the conducting of criminal case investigation — or accordingly tasks DCEC.

Case study 10.3

On May 10, 2021, the MIA of Uzbekistan territorial division detective issued an indictment order for citizen Sh. within criminal case investigation. At 19:10 same-day materials for inclusion in the List were set before DCEC.

Inclusion into the national List was made no later than 10:30 May 11, 2021.

According to the message sending data, notification about List updating was sent to supervisory bodies via an electronic channel at 11:05, while to the CB and to Banks — at 10:49.

At the same time, there were published the updated List, corresponding notifications and information in the accounts on the DCEC website. A message in Telegram was published at 11:03. At the same time, the software product of the FIs downloads the updated List from the website of the DCEC and checks the data of the client base. If there is a match, the assets are frozen.

687. Assessors were provided with examples of national enlisting on grounds other than terrorism-related criminal case investigation (regarding that very person).

Case study 10.4

Based on the MIA information, two terrorist activity-related persons wanted by the police for committing a crime under CC Article 223 ('Illegal exit abroad or illegal entry into the Republic of Uzbekistan') were included into the national List.

688. Should be noted, however, that Provision within the General Prosecutor's order as of September 30, 2016 No. 22-B does not envisage enlisting of persons wanted for other than terrorism- or proliferation-related accusations, that obviously requires making amendments to the regulatory legal act and harmonising it with the existing practice.

689. There have been 5 cases of exclusion from the national List — following FIU monitoring or SSS message.

690. While communicating the updated List to supervisory bodies and reporting entities, DCEC, as a law enforcement type FIU, simultaneously checks information regarding the enlisted person in all databases available (on property, money, and financial instruments). This checkup is made to additionally secure prompt identification and freezing of assets.

691. Besides, in case of identification of a person related to terrorist activity or TF before enlisting, FIU is authorised to issue and forward a prescript of funds and other assets operations suspension (for up to 30 days). That ultimately facilitates the immediate application of TFS. However, there have not yet been such TF and TFS prescriptions issued, as the existing procedure of enlisting ensures prompt TFS application.

Immediate application of TFS by reporting entities

692. The FIs and DNFBPs apply the TFS and implement the freezing of assets immediately after the publication of changes to the List on the website of the DCEC in the personal account. This obligation is stipulated for them in the legal acts.

Case study 10.5. Example of immediate check of the existing client base with the updated List and freezing of funds

On 10.06.2021 at 4.12 pm, the List was updated and communicated to reporting entities due to the inclusion of 15 individuals.

On the same day, before 6 p.m. nine commercial banks submitted reports on suspicious transactions to the DCУC on freezing the funds of 13 individuals for a total amount of 200.6 thousand Soums, 7.5 US dollars and 0.07 Euro. These funds are frozen in the current accounts of the banks' customers, identified by checking the current customer base with the updated List.

693. All FIs receive the list updates immediately after their publishing. It is accessible from several points: online via the dashboard on the FIU website, via a secured line with delivery confirmation and notification in Telegram, and through automatic upload of files in the automated banking system.

694. Fis also use automated systems of sanctions check in parallel. They compare data not only with those in the List and UNSC sanctions lists but with corresponding EU and OFAC (Office of Foreign Assets Control) registers. Data then are uploaded from the designated websites allowing for, essentially, double verification of data being received. Obligation to have automated check systems in banks is envisaged by the Central Bank Board Resolution (2015).

695. While uploading new lists, the existing client database is immediately checked as well. When either onboarding or transacting a client, FIs verify whether that has been enlisted. If matched, they immediately suspend transactions or freeze assets and forward to FIU a report indicating the amount (sum) of the property frozen.

696. In banks there have been developed and applied technical procedures as to transaction suspension, assets and other property freezing, granting access to the frozen property and resumption of transaction of those included in the List.

697. While visiting banks in the course of the on-site mission, assessors have been showcased with examples of automatically generated blocking of transactions at the teller's desk when attempting to make a transaction on behalf of the person enlisted.

Case study 10.6

Commercial bank

A Bank makes use of an automated system of sanction lists checks. They use software developed by 'Intelligent solutions' (Uzbekistan) directed by OSCE and Central Bank, as well as CS B-2 LTD

(Ukraine). Plus, the bank uses the following companies' software: REFINITIV LIMITED (World-Check); Alliance Factors Ltd (Sanctions Screening&KYC Registry). The list of persons suspected of terrorist and extremist activity is embedded into the automated bank system. If a client's data match those in the List, the transaction is immediately blocked (online) and an authorised compliance control staff member receives a notification about the matching.
Particularly, on December 20, 2020, a USD 350 money transfer sent by an enlisted person entered the system. All the identity details have matched. Funds were frozen; FIU was sent a report indicating the amount (sum) of the property frozen.

698. Software systems in all NBCI and payment institutions allow online automated identifying and suspension of enlisted persons' transactions. Thus, having received the updated list, NBFI perform the automated system checkup and if those enlisted are identified NBCI immediately forward a report to DCEC. Having such software available is a licensing requirement of the CB for entities under control.

699. Postal service operators receive the list from DCEC via secured electronic channel of communication. There are three ways of the list receiving: following its entering administrative support office of MITCD, on the DCEC website, account at the said website. Forwarding information via a secured electronic channel takes less than an hour. Postal service operators input data to AML/CFT search system. Notification of the list's amendments being made is performed via news posting on the DCEC website and via Telegram channels.

700. One of the main risks highlighted by the postal sector representatives is that there are postal establishments with the enlisted persons' addresses in their servicing area. This is the reason for the enhanced CDD measures being taken at these establishments.

701. The stock market and insurance sector apply TFS only towards new clients and to financial operations of existing ones. Due to the absence of software layouts, representatives of these sectors are unable to constantly check all their clientele for matching with the updated List in an expedient manner.

702. The exchange has established a fact fixing procedure as to the prompt forwarding of the Lists. At RUACE (Republican Universal Agricultural Commodity Exchange) and at UzEx (Uzbek Commodity Exchange) there has been followed by a practice of their members mandatory Lists reviewing via dashboards. Authorised staff members of the exchange receive the List from the Antimonopoly Committee via the electronic channel of communication. Information is transferred through secure channels. There has been signed a trilateral agreement foreseeing communicating the Lists to the exchange members within 1 hour and 15 minutes.

703. Each and every DNFBP sector has an access to a dashboard on the DCEC website with the latest editions of the Lists. All the sectors receive notifications about Lists updates via the secure electronic channel and additionally via Telegram channel.

704. Also, the notary and real estate agent sectors receive the Lists through sectoral informational systems moderated by supervisory bodies (AIS 'Notary' and AIS 'Valuation and Real Estate Activity'). Information about viewing and downloading the List is available to supervision authorities, too, and if a reporting entity does not use the List, it receives a reminder about the necessity to use phone notifications made by supervisory body representatives. Thus, supervision authorities constantly remotely monitor DNFBP use of the Lists.

705. In case of data matching with the List, the financial or other property transaction shall immediately and without prior notification be suspended, however, DNFBPs have not yet reported the cases, as well as identification of enlisted or acting on behalf of such persons or legal entities in their control.

706. State Assay Chamber under the Finance Ministry representatives has pointed out that received from DCEC List is immediately (with a 3-hour confirmation) communicated to those conducting operations with PMPS via Telegram, and that they also inform them about the publishing of the List on the Ministry of Finance and DCEC websites. Still, the effectiveness of the really taken measures is doubtful, as sector representatives interviewed noted manual routine with hard copies of the List.

707. DCEC representatives have noted work interaction between FIs and FIU also in the sphere of TFS implementation and application. There have been cases of FI staff direct communication with FIU officers on some issues, for example, when data of a person match, but there has been presented different passport. Then the FIU officer checks the data in their databases and communicates with FI. Background on FIU authorised staff members are available to all FIs and DNFBP.

708. According to information provided by the CB, there were 1,037 false positives on the international list in 2016, 1,384 in 2017, 1,928 in 2018, 1,877 in 2019 and 2,063 in 2020.

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

709. The Republic of Uzbekistan takes certain efforts to evaluate and monitor the NPO sector as to potential abuse with TF purposes and applies measures to prevent that.

710. As of June 1, 2021, there were registered 9204 NPOs, including 474 non-governmental foundations and 2308 religious organisations (2098 mosques and 210 others). As more than 90% of the Uzbekistan population practice Islam, namely Islamic religious organisations receive more cash donations compared to those of other confessions.

711. On the basis of the NPO definition from the interpretive note to the FATF Recommendation 8, in the Republic of Uzbekistan NRA, the country has made a conclusion about the obligatory character of the TF risk mitigation measures to be taken towards non-governmental foundations and religious organisations. The Ministry of Justice following their analyses of the NPO sector (SRA) have rated non-governmental foundations and religious organisations as those having an average level of risk. Due to the recent adoption of the PRA report, there has been no update.

712. Financing from abroad appears to be a risk-growing factor in terms of using NPO for TF purposes. However, NPO representatives having met with assessors noted a decrease in the amount of NPO foreign financing because of more proactive state support of NPOs.

713. For the most part, measures taken by competent authorities to prevent the possible use of vulnerable NPOs for TF purposes are general measures that apply to all types of NPOs. However, the existing uniform regulatory and supervisory measures are proportionate and may cope with the current risk of NPOs being used for TF purposes.

714. This is supported by the fact that no instances of religious organisations being used for TF purposes were identified in the course of inspections carried out by the MJ to mitigate the risks of NPOs being used for TF purposes.

715. Nevertheless, there are also some targeted measures that are applied exclusively to NPOs requiring the mandatory application of risk mitigation measures for TF purposes.

716. As a general measure, where there is clear and demonstrated evidence that the NPO being established is intended to be used for TF, a mechanism for denial of registration may be used. Before determining whether an NPO can be registered or receive assistance from foreign governments, international organisations, etc., or to accredit NPO staff, the MJ submits materials for review to certain government agencies and organisations and receives their opinion within 20 days. If there is convincing evidence that the purpose of an NPO's registration is to advocate war, social, national, racial or religious hatred, or to harm the health or morals of citizens, its registration may be refused.

717. When registering new NPOs, their managers must be given a signed acknowledgement of all obligations stipulated by the legislation, including those related to AML/CFT.

718. Justice Ministry and National Association of Non-Governmental Non-Profit Organisations have adopted the Standard on Transparency of Non-Governmental Non-Profit Organisations Activity, encompassing a set of measures aiming at ensuring openness, legitimacy, non-corruption, accountability, as well as sustainability and effectiveness of operations and management for securing transparency of NPO activity.

719. The transparency standard includes a set of measures aimed at ensuring openness, legality, freedom from corruption, accountability, and a reliable and efficient style of operation and management.

720. In accordance with the Standard, NPOs shall post on their official website and on the website www.e-ngo.uz information on the following: (i) property, donations received during the financial year, sponsorship funds, contributions, subsidies, grants and other income, including funds from foreign sources and their sources; (ii) ongoing projects (programmes and others) and their results; (iii) events held by the NPO (meetings, meetings, conferences, briefings, workshops, round tables and others); contracts (transactions) concluded, including with counterparties; (iv) business income (profit); (iv) expenses related to activities (administrative and other expenses); (v) list of persons connected to the NPO, in particular to the public fund, changes in them; (vi) members of NPO governing bodies, members of the board of trustees, management board and the audit committee of public funds as well as changes in them; (vii) decisions taken in relation to activities and not prohibited for public disclosure.

721. The accuracy of reports submitted to the justice, state tax and state statistics authorities may be compared with data published as part of the transparency standard.

722. The Standard distinguishes three levels of transparency depending on the amount and completeness (relevance) of the information posted: (i) basic transparency; (ii) medium transparency; (iii) full transparency. The level of basic transparency indicates that the NPO is actually carrying out its activities. A medium level of transparency provides full information about the NPO's activities and means that the NPO has sufficient experience in performing its socially relevant functions. A level of full transparency means that the NPO is transparent and open and that its business style and management are robust and effective.

723. This is practically realized through the publication of information constituting each level of transparency on the official website of NPOs and the website www.e-ngo.uz.

724. The MJ, as an authorized competent government body, monitors NPO activity and also attends events held by NPOs.

725. Prioritisation of monitoring of specific NPOs is based on two factors: doubts as to the performance of the declared activities or suspicions of illegal activities and the volume of incoming funds. However, the fact that an NPO is classified as one requiring mandatory application of TF risk mitigation measures is not considered as a basis for priority monitoring of activities due to the inappropriateness, according to representatives of the MJ, of unwarranted interference in the NPO's ongoing activities. This means that the country understands that the measures taken should not interfere with and disrupt the legitimate activities of NPOs.

726. As a general measure to mitigate the risk of NPOs being used for TF purposes, a list of individuals involved in terrorist activities could be made available to NPOs. However, the Ministry of Justice does not make the List available to NPOs. According to the Ministry of Justice, the reason for this is that NPOs are not institutions involved in transactions with funds or other assets. Consequently, the MJ has no obligation to provide them with the List. The List of persons involved or suspected of involvement in terrorist activities is taken into account by the MJ and taken into account in the monitoring process of the NPOs' activities.

727. A standard risk mitigation measure for NPOs is to raise awareness amongst NPOs of their potential use for TF. During 2015-2019, over 50 workshops and over 200 outreach events were conducted on compliance for NPOs, particularly on preventing extremist and TF-related transactions in their activities, to explain the legal requirements and international standards for TF. Typically, seminars are held on the following topics: "prevention of terrorism and extremism and their negative aspects"; "terrorism and extremism risks and methods", etc. NPO officials, accountants and other representatives of NPOs are the target audience for these seminars.

728. Sometimes, representatives of FIU and LEAs participate in such informational and explanatory events.

Case study 10.7
In 2020, the Ministry of Justice held a workshop for NPO representatives on combating the legalisation of illegal proceeds and financing of terrorism using NPO and on the interaction between NPOs and governmental authorities.
Representatives of DCEC have also attended the workshop.
During the workshop the followings have been discussed: the FATF Recommendations (their essence, meaning and implementation); national risk assessment of legalisation of illegal proceeds and financing of terrorism when it comes to the risks of NPOs' use for TF purposes; internal control over raising and putting of cash to NPO banking accounts; proper use of donations by donees; specific aspects of donees' identification (use of open sources: the List of individuals involved into terrorist activity or suspected of, list of terrorist organisations); NPO obligations as to combating the financing of terrorism.

729. Specifically targeted control measures envisaged for public foundations, which have been identified as requiring mandatory measures to mitigate the risks of use for TF purposes, are their obligation to publish annual reports on their activities and conduct an annual audit. The reports of public foundations are posted on the MJ's Non-State NPO Portal, which can be accessed through the website www.e-ngo.uz.

730. Another targeted measure to reduce the risks of using public foundations and religious organisations for TF purposes is to ensure transparency and control over fundraising, primarily the accounting of donations.

Case study 10.8. (NPO Non-governmental charitable foundation 'V.')
According to the Law on Freedom of Conscience and Religious Organizations Article 8, a centralised Department of Muslims of the Republic of Uzbekistan has been established to coordinate and direct Muslim religious organisations' activity over the country.
Under the Department of Muslims of the Republic of Uzbekistan there has been formed NPO Non-governmental charitable foundation 'V.' whose main tasks are building, repairing and reconstruction works, landscaping, and maintenance of mosques and religious organisations, as well as material and social support of people working at mosques and of places of pilgrimage, too.
To effectively control the incoming foundation accounts cash turnover, in June 2018 DCEC under GPO, the Committee for Religious Affairs under the Cabinet of Ministers, the Justice and the Culture ministries, STC, Central Bank, Department of Muslims of the Republic of Uzbekistan, State Council for Coordination of Self-Government, as well as other organisations have adopted a joint resolution.
According to it, all cash entering charity boxes on the territory or near mosques, places of pilgrimage and cultural sites should be put on the foundation and corresponding mosques banking accounts under the control of the working group consisting of the abovementioned bodies' representatives. Moreover, on January 19, 2021, the Department of Muslims of the Republic of Uzbekistan adopted an order regulating (additionally to the joint resolution mentioned) the quantity of the charity boxes as well as their maximum distance from mosques and places of pilgrimage. While opening, charity boxes may be video recorded.
Foundation representatives have confirmed their adherence to the donation collection and record-keeping procedure and have pointed out that the report on their expenses is published on the foundation's website regularly (on a daily basis).
While considering appeals for help, they identify people via their passport and the official document from the local territorial administration ('viloyat'). Funds are put on banking card accounts only or are transferred to the respective seller in case of goods purchasing.
The foundation does not verify card accounts spendings as per their intended purpose.

731. Ensuring control over the expenditure of funds by public foundations and religious organisations is also a targeted measure. Cash assistance is not provided to NPOs. Helping funds are transferred to a bank card, generally not exceeding USD 100 per year per applicant.

732. Big foundations, such as Charitable Public Fund "B" at the Administration of Muslims of Uzbekistan, have their own billing system, which allows tracking monthly receipt of funds with breakdown by types (charity, zakat, fitr, actions, places of pilgrimage, etc.) and ways of receipt (banking services, payment systems, info-kiosks and system "Munis"), as well as daily and monthly distribution of

received funds in the context of purposes, for which they are directed, on the website (https://vaqf.uz/uz/transactions/statistics) of this organization, including charity. The system indicates the name, address, contacts of the recipient, the amount and purpose of spending money (carrying out planned and unplanned medical operations, improving the financial situation of persons, etc.). In addition, this foundation's website contains information about existing and completed charitable projects, with information about the amount of required, collected and spent funds.

733. One form of control over the targeted use of funds received is the unified interactive portal "Transparent Charity" (http://shaffofxayriya.uz/uz), which allows centralised accumulation and distribution of charitable donations, monitoring their targeted and targeted use, ensuring full automation and transparency of these processes, and enabling charities to trace the use of their funds. But it's working in the test mode at the moment.

734. In addition to identifying NPOs at risk of TF, and applying specific targeted measures to them differently from those generally applied to all other NPOs, there are also differential measures applied to different types of vulnerable NPOs, i.e. there are a number of measures that apply to public foundations but do not apply to religious organisations.

Table 10.6: Differentiation of measures applied to vulnerable NPOs depending on their type.

Regarding public funds	Regarding religious organisations
Funds are subject to a mandatory annual audit An audit committee shall be established to supervise the financial activities and the proper use of the money and other assets of the fund Annual publication of the report The foundation has no right to enter into transactions with or perform other actions for the benefit of persons related to the foundation if (Article 23 of the Act): - such transactions or actions are carried out on more favourable terms than with persons who are not related to the foundation; - a person related to the foundation is a member of the board of trustees of the foundation. The annual aggregate amount of the administrative costs as well as the remuneration and compensation of the members of the board of trustees and the audit committee related to the performance of their functions shall not exceed twenty per cent of the total expenditure of the foundation. Charity funds are obliged to: - keep records of charitable donations received; - disclose information about charitable donations received within ten days of receipt in the media and, if available, on their official websites. The charity fund provides access to its annual reports. Information on the amount and structure of the charity's income and expenditure, assets, number of employees, their remuneration and the involvement of volunteers is not a commercial secret.	Registration requires an opinion from the Committee on Religious Affairs under the Cabinet of Ministers of the Republic of Uzbekistan Registration requires the opinion of the local executive authorities (the Council of Ministers of the Republic of Karakalpakstan, the regional khokimiyats and the city of Tashkent) A document of religious professional education of the head of a local religious organisation is required for registration, with the exception of denominations whose doctrine does not provide for a system of religious professional education.

735. In addition, there are also differentiated measures for vulnerable NPOs of the same type, depending on the degree to which they are more or less likely to be used for TF purposes, such as the frequency of monitoring and inspections, as well as visits to such NPO activities. Such measures apply, for example, to different types of religious organisations.

736. Assessors note the significant number of measures envisaged, both general and targeted. Based on the meetings with the representatives of the MJ, the assessors concluded that the existence of such a large number of measures allows the Republic of Uzbekistan to have a differentiated approach to

determining the set of required measures, depending on the degree of risk of the NPO concerned. This means that with respect to a number of NPOs, the country may limit itself to more lenient measures in the case of a lower risk of involvement of such an NPO, and, conversely, determine more significant measures with respect to more risky NPOs.

737. Assessors consider that NPO representatives having participated in their meetings sufficiently understand the vulnerability of those organisations as to their being used for TF purposes, but do not pay particular attention to the appropriate usage of the support received — because they think that this issue is covered by a bank when opening a card account for receiving funds by a needy person.

738. FIs are also involved in mitigating the risks of using high-risk NPOs for TF purposes, as evidenced by the statistics of STRs directed to NPOs.

Table 10.7. Statistics on NPO-related reports from FIs to FIU

Year	Total quantity of messages	Where		
		Foundations	Religious organisations	Other (trade unions, associations, federations, etc.)
2016	365	85	3	277
2017	219	42	1	176
2018	154	47	2	105
2019	108	48	1	59
2020	179	68	9	102
Total	1 025	290	16	719

739. All STRs related to the activities of religious organisations and foundations were sent in connection with the expenditure of funds by these NPOs.

740. With this in mind, the assessors believe that a deficiency in the system of both general regulatory measures and specific targeted measures for high-risk NPOs is the lack of control over the targeted use of the submitted helping funds. The Ministry of Justice limits itself to NPOs reports on the receipt and expenditure of funds. The NPOs themselves consider it impossible to control the intended use due to a lack of appropriate authority, relying on CDD measures, conducted by banks when opening a bank account. Nevertheless, factors that significantly reduce the risk in this situation are the small amount of assistance provided and its disbursement in non-cash form.

741. As it has been noted in the Recommendation 8 Technical Compliance report, a wide range of sanctions can be applied for breach of law in the sphere of NPO activity. There have been no cases of sanction applications relating to NPOs' involvement in TF.

Case study 10.8

DCEC has received an STR from the banking sector regarding citizen A.'s cashing in funds from the account of a mosque (where he is the imam) for 450 million Uzbek sums, as well as converting cash at the cash-desk (USD 94.4 thousand and USD 9.7 thousand).

In the course of financial analysis, there has also been identified a banking card of A. where he received funds from other cards belonging to various persons for a total of 450 million Uzbek sums.

Following the analysis, relevant information was prepared and forwarded to the DCEC under GPO and SSS territorial divisions for according checkups.

During a joint review by DCEC staff members and the Department of Muslims of the Republic of Uzbekistan, there has been established that while mosque renewal, A. (to enlarge the mosque's territory and build additional premises) pursued to purchase of a neighbouring site (house), for which he organised raising of funds to his banking card and then converted them together with the funds withdrawn from the mosque's account as the site owner required USD cash payment for his site.

742. The MJ representatives did not indicate whether and how they use the data provided by the FIU on the results of the OIMs in relation to individual participants, organisers of NPOs, analysis of STRs received by the FIU related to NPOs, etc.

743. There is no direct interaction between the FIU and the NPOs, according to NPOs representatives. The main control activities are carried out by the Ministry of Justice (regulator), SCC and CB.

744. No requests related to NPOs, including information on the dubiousness of foreign donors to NPOs, were received through international cooperation channels.

745. In light of the information received, the assessors believe that significant proportionate measures are applied to vulnerable NPOs, both general and targeted. Applying these measures together addresses the existing risk of NPOs being used for TF purposes, as evidenced by the absence of such instances in the high level of TF risk identified in the NRA. Specific controls are used in accordance with the RBA, while general controls are applied within a unified regulatory and supervisory framework.

746. While inadequate monitoring of the intended use of helping funds is a weakness, is mitigated significantly by the use of non-cash settlements and the involvement of FIs in mitigating the risk of using NPOs for TF.

Deprivation of TF related assets and instrumentalities

747. The Republic of Uzbekistan has demonstrated that it deprives terrorists, terrorist organisations and terrorist financers of their assets and means of crime committing via taking various measures, including enlisting and assets freezing. Although the total amount of frozen assets is not large, it corresponds to the risk profiles as those frozen assists owners who use, as a rule, their own sources of income and not third-party financing, represent relatively poor strata of the population having restricted access to funds.

748. Freezing of enlisted persons' assets was carried out only by financial organisations.

Table 10.8. Statistics on assets freezing and granting access

Year	Amount of freezed funds			Amount of funds granted access to
	Uzbek sum, mln	USD	euro	
2017	3.4	3 375	9	
2018	4.5	200		USD 200
2019	19.0			
2020	6.6	6 100		USD 1 300
6 months of 2021	17.6	298.3	0.07	

749. Almost all individuals from the list are abroad now. The main cases of assets freeze relate to the counterparties of the corresponding financial organisations, not to their clients.

Case study 10.10

On June 26, 2020, citizen Zh. was included in the List for his involvement in terrorist activity. On July 27, 2020, he transferred USD 400 to citizen T. via money transfer system (further — MVTS) from Russia. When T. in bank 'A' for receiving, its staff members put a hold on her operation and froze the funds.

Moreover, on August 28, 2020, Zh. transferred USD 300 to citizen Sh. from Russia via MVTS. When Sh. came in bank 'B' for receiving, its staff members put a hold on her operation and froze the funds.

From above it is seen that in the second case the money was intended to be received by another person at another bank — maybe it was an attempt to evade asset freezing measures.

750. As it has already been mentioned, there were no cases of up-to-30-day funds or other property operations suspension, so, there are no statistics as to the amounts of assists frozen through this mechanism.

751. During the timeframe under review, there have been cases of granting access to the frozen property for covering of essential life needs.

Case study 10.11

On October 3, 2018, citizen P. was included in the List for his involvement in terrorist activity. On May

21, 2020, he transferred USD 250 to his sister H. from Turkey via MTS. When H. came to the bank for receiving, its staff members put a hold on her operation and froze the funds.
On May 21, 2020, H. appealed for granting access to the frozen funds for covering her parents' essential life needs (food, pharmaceuticals, utility payments), with copies of backup documentation.
Following the appeal review (June 4, 2020), the body having submitted materials for P.'s enlisting made a decision to grant H. access to the frozen USD 250.

752. Although most terrorism financing cases involve the transfer of funds abroad and the financing of travel, confiscation of funds intended for TF does occur.

Table 10.9: Information on confiscation of funds intended for TF (or their equivalent)

	2016	2017	2018	2019	2020
Amount of confiscated funds (in million UZS/USD)	6,2 / 2,197	2,9 / 900	854,7 / 105,027 (*equivalent)*	8,2 / 750	0

Consistency of measures with overall TF risk profile

753. According to NRA, the Republic of Uzbekistan has a high TF risk level.

754. On the whole, taken by the Republic of Uzbekistan government measures conform to the country's overall TF risk profile. Uzbekistan regularly enlarges the List not only making the inclusion of persons from UNSC sanction lists and domestically identified terrorist activity related ones but constantly exchanging the lists with other states as well (mutual freezing of assets).

755. The country pays attention to the transparency of NPO activity, the NPO measures used in the NPO package deal with the existing risk of NPOs being used for TF purposes.

756. Assessors have been provided with information on having at competent authorities' disposal resources that seem to be adequate for performing duties related to TFS implementation and application while working with NPOs.

Overall conclusions on IO.10

757. The Republic of Uzbekistan recently (for 2 years) had a coherent system for the implementation and application of the TFS, which allows the FIU to timely include the designated persons in the List, and the reporting entities to freeze assets immediately, indicating the TFS regime is acting "without delay". In previous years, the system hadn't fully implemented the "without delay" principle.

758. The lack of cases where the Republic of Uzbekistan has submitted proposals for inclusion on the UN Security Council sanctions lists may be a disadvantage, given the large number of individuals on the national section of the list.

759. Both general and targeted significant proportionate measures to vulnerable NPOs are applied in the country. Specific controls are used in accordance with the RBA, while general controls are applied as part of a unified regulatory and supervisory framework. Applying these measures together permits coping with the existing risk of NPOs being used for TF purposes.

760. Although the insufficient control over the intended use of helping funds is a weakness, it's significantly mitigated by the use of non-cash settlements and the involvement of FIs in the risk mitigation processes of using NPOs for TF purposes.

761. Uzbekistan seeks to deprive terrorists, terrorist organisations and individuals who finance terrorist activities of their assets and the means to commit crimes through various methods, including designation, freezing of funds and confiscation as part of the investigation and prosecution of TF cases.

762. The measures taken by the Uzbek authorities are generally consistent with the overall TF risk profile of the country.

763. **The Republic of Uzbekistan is rated as having a substantial level of effectiveness for IO.10.**

Immediate Outcome 11 (PF financial sanctions)

764. The Republic of Uzbekistan does not have common borders with DPRK and Iran. Despite diplomatic relations established, there is no DPRK embassy in Uzbekistan; mutual trade for the first six months of the year 2021 has been less than USD 365 000. Uzbekistan-Iran trade is also insignificant: for the first six months of 2021, the exports were at USD 104 million (less than 1.5% of the total exports of Uzbekistan) and included mainly cotton, silk, fertilisers, fruits and vegetables. Imports from Iran were at about USD 91 million (0.8% of the total imports)[55].

765. The Republic of Uzbekistan is not either a large international or regional financial centre, as well as it does not have well-developed marine insurance sectors. However, it has manufacturers of goods and materials that could possibly be used in the WMD (weapons of mass destruction) sphere. Particularly, Uzbekistan is at 11th place in the world in terms of uranium resources and at 5th place in terms of their mining[56]. In addition (although it falls outside the scope of this evaluation report), the Republic of Uzbekistan has a mode of export and customs control over the corresponding goods trade in place ensuring conformity to the UN sanctions, as well as it takes controlling measures towards main financial operations presumably related to WMD proliferation. According to information from the country's competent authorities, there have been no cases of dual-use goods trading with Iran or the DPRK.

766. In the overall context, there are no unbiased prerequisites for use of the Uzbekistan territory for proliferation financing activity.

767. An Iranian bank (100 percent foreign ownership) functions in Uzbekistan, its main goal is the development of Uzbekistan-Iran trade partnership relations. Plus, the bank serves Iranian citizens working or living in the Republic of Uzbekistan. According to the UNSCR 2231 (2015), starting from January 16, 2016, the Security Council's sanctions should not be applied to this financial organisation. As of 01/01/2021, the total number of customers of the bank was 1,285. For client checking, additionally to regular and enhanced procedures, the bank uses diplomatic channels as sources for extra information receipt. The Iranian bank itself is currently under enhanced monitoring by the Central Bank of Uzbekistan as part of its risk-based supervision. Enhanced monitoring involves more extensive and in-depth analysis by increasing the frequency of reporting and/or establishing additional reports. In particular, for monitoring purposes, the financial institution provides the Central Bank with monthly information on customers and their activities; information on export and import contracts and cross-border bank transfers; and information on high-risk transactions. As the bank does not offer a range of banking products and services and has AML/CFT internal control and while its clientele is of insignificant quantity, the risks related to its functioning assessors have been evaluated as low.

Implementation of targeted financial sanctions related to proliferation financing without delay

768. Assessors have found that lately in the Republic of Uzbekistan acts a largely effective system of implementing TFS related to PF. Since there is a single procedure for the implementation and application of TFS for both FT and PF, all of the provisions of IO10 to the full extent apply to the TFS regime for PF.

---

[55] State Committee of the Republic of Uzbekistan on Statistics/Foreign Trade https://stat.uz/ru/ofitsialnaya-statistika/merchandise-trade

[56] World Nuclear Association: World Uranium Mining Production https://www.world-nuclear.org/information-library/nuclear-fuel-cycle/mining-of-uranium/world-uranium-mining-production.aspx

769. According to current the Republic of Uzbekistan legislative requirements, MFA informs DCEC on sanction lists drafted by UNSC Committees once available through official channels. However, since this method did not meet the without delay requirements, the authorities introduced a procedure for updating the List by having in the FIU 24/7 working employees responsible for the TFS. Information received through the MFA channels is used, however, by nature that represents an additional tool for the verification of already adopted changes to the List and the application of the TFS. The FIs and DNFBPs apply the TFS for the PF and freeze assets immediately after the publication of changes to the List on the website of the DCEC in their personal account.

770. DCEC is a competent authority responsible for PF-related person list drafting, maintenance and bringing it to the knowledge of supervisory bodies and reporting entities like they do in the case of the TF list. The Republic of Uzbekistan can implement TFS not only pursuant to the PF UN sanction lists but within the framework of the national regime, too, — and they can freeze assets of those related to PF in response to third-country enquiries. Currently, the list consists of persons enlisted by UNSC in accord with PF Resolutions.

771. Competent authorities and the private sector have demonstrated that in practice (at least, during the last 2 years) they took measures as to timely inclusion of those related to the PF into the List and communicating it to the organisations dealing with funds and other property and as to freezing as well. ”Without delay” principle is preconditioned by DCEC authorised officers’ regular monitoring of UN Security Council press releases and alterations in the corresponding lists on the UNSC website as well as by use of up-to-date electronic channels for communicating the List to the reporting entities[57]. Particularly, the last update of the UNSCR 1718 sanction list (alteration of one entry) took place on May 11, 2020, and on May 12 already the corresponding Republic of Uzbekistan List was updated and brought to the reporting entities’ knowledge.

772. Relying on the data showcased, assessors come to the conclusion that such a coherent system of TFS implementation and application functions for the last two years. In the earlier period, experts believe that the system operated within the time frame described in the TC, i.e. it did not fully enforce the "without delay" principle.

773. At the time of the on-site mission, there were 239 persons in the PF part of the List (DPRK: 80 individuals and 75 organisations; Iran: 23 individuals and 61 organisations), that fully corresponds to the UN PF sanction list. The List is publicly available on the DCEC website (http://new-department.uz/ru/about/documents/), published in the reporting entities’ accounts on the DCEC website and communicated to supervisory bodies (including CB) and to the banks via specialised electronic channels of communication. Notary and real estate agent sectors, also, receive the List through sectoral informational systems administered by supervisory bodies. Plus, reporting entities are notified in sufficient time in advance via Telegram group messaging on any alterations made to the List.

774. The Republic of Uzbekistan has the interagency procedure of considering individuals and organisations inclusion (MFA being a coordinator) to the UN sanction lists according to Resolution 1718 (on DPRK) and 1737/2231 (on Iran) and succeeding in place. In case of identification of or receiving information on a person to be included in UNSC Committees sanction lists, competent authorities of the country forward the data to MFA for their further forwarding to be reviewed by the corresponding committee; at this, the information has to be agreed with the SSS. Competent authorities interact within the framework of existing mechanisms of interagency cooperation based on agreements in force and general provisions on interaction. When received, MFA review the information for sufficient grounds for a person’s being eligible for UNSC enlisting, for the availability of complete identity details and designated by the UNSC Committees record forms

[57] After the on-site mission the country adopted amendments to the legal acts, regulating the order of implementation and application of the TFS (Order of the Prosecutor General of the Republic of Uzbekistan № 53-B dated 30.07.2021), which corrected the deficiencies noted in Recommendations 6 and 7 in terms of compliance with the principle of "without delay" application of the TFS.

filled in. Extra information is requested if needed. Up to now, this procedure has not been practically applied.

775. Resolution on freezing (2016) also foresees procedures and grounds for excluding from the List, appealing against the enlisting (via addressing FIU in written form and in case of refusal — via reference to the court), renewal of the suspended operations and granting access to the frozen assets.

776. It is necessary to notice that during the on-site mission, there has been adopted a joint agreement on interagency cooperation in the CPF sphere[58] between DCEC, SCC, SCIS, and Central Bank. Although this measure is a novelty, assessors during their meeting with authorities' representatives have made sure that SCC and SCIS earlier used in their work the PF List received from DCEC. Specifically, SCC makes consultations with the PF List while monitoring the movement of goods and funds across the Uzbekistan border and SCIS do so when licensing activity in the sphere of nuclear energy use. Besides, SCIS regularly forward actual data on the import of corresponding goods to DCEC for reviewing.

777. As it has been noted in R.7, the obligation as to funds and other assets of PF-enlisted persons freezing does not relate to all individuals and legal entities, but only to reporting entities, as there are no provisions directly envisaging liability for all physical and legal persons for breach of this prohibition (except for FIs and DNFBPs). Therewith, the Republic of Uzbekistan citizens and legal entities, foreign citizens and legal entities, persons without citizenship and those acting on behalf of all categories mentioned are prohibited for providing direct or indirect access to money or other property, material resources, financial and other services to persons included into the List within the territory of the Republic of Uzbekistan. From the effectiveness point of view, in the Republic of Uzbekistan, there have been no cases that could have demonstrated the possibility of application of sanctions to an individual or legal entity in breach of requirements on TFS application according to the UNSC Resolutions 1718 or 2231.

778. In addition to the PF TFS measures mentioned above, the Republic of Uzbekistan has an efficient customs and export controlling system, one of its duty being control over dual-use goods turnover (with the engagement of the MFA, SCC, SCIS, and MIFT. According to the Republic of Uzbekistan Law on Export Control as of August 26, 2004, No. 658-II, MIFT is an authorised state authority in the sphere of export control and also has powers to issue corresponding export permits. By the President of the Republic of Uzbekistan Decree as of November 3, 2017, No. UP-5215 'On regulative measures as to licensing of specialised goods export and import as well as to registration of export contracts and expert reviewing of import ones' there has been adopted a list of specialised goods, export and import of which should be licensed based on the President of the Republic of Uzbekistan or CM decisions. Control over regulated export items outflow and usage also encompasses written obligation regarding those items non-usage for manufacturing of weapons of mass destruction and of corresponding delivery means as well as other kinds of weapons and military equipment. MIFT also has direct access to the SCC automated system for control over the cross-border movement of goods.

779. SCIS is the authorised body of state governance responsible for the implementation of unified state policy and control over ensuring radiation and nuclear safety at nuclear infrastructure and in the sphere of nuclear technology and industrial safety at hazardous production facilities[59]. Since 2015, the SCIS Chair has been a head of the Regional Secretariat of Centres of Excellence on mitigation of chemical, biological, radiological, and nuclear risks for Central Asia aiming at the promotion of regional cooperation for raising awareness, readiness and potential in the sphere of CBRN-risks mitigating at national, regional and international levels.

780. Resolution of the CM of November 27, 2018, No. 968 has established the National Action Plan of the Republic of Uzbekistan on implementation of international documents on ensuring chemical,

[58] Approved by Department for Combating Economic Crime under General Procecutor's Office, State Customs Committee, State Committee on Industrial Safety, Central Bank of the Republic of Uzbekistan as of June 22, 2021 No. 25, 01/24-2085, 360-B

[59] Regulation on the State Committee on Industrial Safety of the Republic of Uzbekistan adopted by the Resolution of the Cabinet of Ministers as of February 1, 2019 No. 75

biological, radiological, and nuclear safety for 2018–2021 years, aimed, among other goals, at the adoption of an updated list of regulated export goods and timely and effective performing of other tasks on ensuring of chemical, biological, radiological, and nuclear safety. Now the Plan is at its finalising stage; a similar document is being adopted for the next three years.

781. Besides, SSS conduct OIM and detective operations aimed at taking control over the movement of dual-use goods while SCC receives (and analyse) online information on such goods outflow abroad. Therewith, they consult PF List received from DCEC and identify the environment (relationships) of persons under examination.

782. Also, Uzbekistan takes preventive actions within the framework of countering WMD proliferation. Thus, in November 2019 there was conducted counter-terroristic chemical and biological "Jeyran" field exercise where they trained interagency coordinated interaction of state bodies in case of terrorist threats related to the use of chemical and biological weapons.

783. Assessors have been provided with the example related to potential non-observance of export customs regime showing coordinated efforts of government authorities aimed at identification and stopping non-financial sanction evasion cases. Therewith, it should be noted that these measures fall outside the FATF Standards.

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

784. Assessors have found that the Republic of Uzbekistan has an effective system of enlisted persons' financial and other assets identification and use prohibition in place.

785. Since 2016, funds and other assets operators must: (i) check transaction participants as to their having been included in the list of persons involved in or suspected of proliferation; (ii) immediately and without prior notification suspend the transaction, except in cases of incoming funds entering a legal entity or an individual account; and/or (iii) freeze funds or other property of persons included into the list of those involved into or suspected of proliferation; and (iv) forward a suspicious transaction report to DCEC. Moreover, monetary funds or other property operations must be suspended and money or other property must be frozen if: (i) one of the participants is acting on behalf or by order of the enlisted person; (ii) monetary funds or other transactional assets entirely or partially belong to the enlisted person; (iii) participating legal entity is owned or controlled by an individual or a legal entity enlisted. Over the reporting period, there have been no cases of financial operations and other assets of PF-related persons subject to freeze.

786. According to the Central Bank Board Resolution No. 37/I as of December 26, 2015, banks have been tasked with further enhancing a mechanism allowing for online identification of persons involved in or suspected of terrorist or proliferation activity and taking the appropriate measures by means of new technologies. Moreover, in their informational letter as of August 26, 2019, Central Bank has additionally explained to reporting entities their obligations as to TF and PF TFS application and has tasked all the banks, pawnshops and microcredit organisations with submitting information on working principles of software allowing for online identification of enlisted persons, as well as on repeated clients and all kinds of operations checkups carried out (for cases of their matching with information in the List).

787. As it is noted in IO 6, reporting entities can regard STR depending on the nature of the crime suspected. Over the 2016–2020 years, DCEC received 1784 reports from FIs on operations supposedly Iran-related (PF), for the total amount of USD 39.6 mln, euro 6.0 mln, UZS3.6 bln, and RUR 576.1 mln. The majority of national currency operations relates to salary and dividend payments to staff members or to founders having the Islamic Republic of Iran citizenship. The majority of foreign currency operations were carried out under export and import agreements or as visa fees or salary payments to foreign establishments, embassies and consulates staff (etc.). There also have been cases of SWIFT money transfers between individuals, however, over the 5 years, they constitute less than 2 percent of the total amount of operations. There have been no DPRK-related STR registered.

788. As an additional measure in case of PF suspicion arising prior to enlisting, DCEC may suspend operations for up to 30 working days via issuing a corresponding prescript. There have not yet been real cases of this procedure application relating to PF, among other grounds, because Uzbekistan is able to complete the process of enlisting promptly enough.

789. Additionally, SCC analyses all cross-border transactions related to the movement of goods abroad. Since June 2021, in case of suspicion relating to involvement in PF (or relevant information received) they can detain and confiscate cash and other property being moved across the customs border[60]. At this, SCC also consults with the PF List received from DCEC. Noting that this is a novelty, SCC has not yet applied this procedure.

FIs, DNFBPs and VASPs' understanding of and compliance with obligations

790. As it has been noted in IO.10 and IO.4, FIs sufficiently understand their obligations to TFS application. At the same time, the understanding of the TFS obligations among the DNFBPs is heterogeneous.

791. Financial institutions supervised by the CB use specialised software allowing for the automated search of enlisted persons; and while new lists are uploading, the existing customer base is being checked. In the banking sector, there have been cases (all being CTF-related) of assets freezing because of customer data matching with those in the List, two cases of unfreezing and several examples of granting access to the frozen assets for covering essential life needs — that (subject to procedural equivalence) can be perceived as evidence of to-be efficiency of PF TFS system. The Republic of Uzbekistan also identified persons for whom "false positives" have occurred under the PF TFS measures. Alongside that, some DNFBP sectors with not so sophisticated means of control check their customer bases manually using hard copies of the List.

Case study 11.1 (An example of a "false positive" due to an overlap with the UNSCR 1718 list in a commercial bank transaction)
On February 3, 2021, the system issued a signal that the data of the sender (counterparty) named Song Dol on a money transfer of 123 US dollars matched the data of persons from the International List (KPi.014, KPi.030, KPi.056, KPi.058, KPi.075, KPi.077, KPi.078) and blocked the operation. The Internal Control Service processed this information and determined that it was a false match, as only part of the name (Song) coincided, the rest of the name and other data of the transaction participant did not correspond to the identification information of the persons from the List. After that, the Internal Control Service authorized the transaction.

792. Model internal control regulations (ICRs) on AML/CFT/PF for monetary funds and other property operators have been drafted and adopted by corresponding controlling, licensing and registering bodies together with DCEC. This ICRs have established procedures for the identification of funds and other property of enlisted persons and post-identification activity protocol. Therewith, ICRs for a range of sectors (stock exchange members, notaries and lawyers, real estate agents, leasing organisations, expert members of the securities market, operators, postal service providers, underwriters, and insurance intermediaries) have been updated while on-site mission. All private sector organisations have participated in the meetings while on-site mission and have been aware of their duties regarding the PF TFS application, including the need to perform customer checks as to match with the data on the List (they also knew the date of the last update of the List). Besides, the reporting entities have been aware of the need to suspend operations for up to 30 working days when the corresponding DCEC prescript is received.

793. In Uzbekistan, freezing requirements are also applicable to virtual assets. Although the country has not yet had cases of PF-related freezing of VAs, it has experience of such assists seizure within the

[60] Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 402 as of June 29, 2021

context of other predicate offences. To add, in June 2021, there have been adopted ICR on VA turnover with corresponding requirements on Pf-related TFS.

794. Correct identification by FIs and DNFBPs of the customer's (or the contracting parties) ultimate BO appears to be the hallmark of the PF TFS application process. As it has been noted in IO 4, practically all the FIs understand the importance of identification (and identifying) BO. The most effective mechanisms have been demonstrated by the banking sector representatives who successfully identify the ultimate BO of their customers. Within the CDD framework, the procedure is carried out by FIs using information received directly from a client, while for data verification and for additional review governmental and commercial (World-Check and others) databases are used. If there are doubts about whether the controlling share owner is the beneficiary owner, the bank affirms or disproves this in the course of the customer's transactions analysis. In the banking sector, there have been cases of refusal to serve customers on the grounds of the impossibility to identify the client's beneficiary owner.

795. DNFBPs have different approaches to BO identification procedures. Some of them to a great extent rely on a proprietary right criterion and also identify the beneficiary owner only when the client is a legal entity. All these can negatively influence the effectiveness of TFS implementation because of possible sanction evasion via false legal entities. Out of all Uzbekistan DNFBP categories, the most efficient in terms of BO identification and information collection are notaries and lawyers (see IO.4). The the Unified State Register of Economic Subjects is mainly used for collection the information.

Competent authorities ensuring and monitoring compliance

796. In the course of the on-site mission, assessors were satisfied that the Republic of Uzbekistan competent authorities monitor and to a great extent ensure performing by reporting entities of their obligations on PF targeted financial actions. The country has demonstrated effective approaches to the private sector informing of the AML/CFT/PF requirements and related risks.

797. Central Bank regularly examines the supervised entities regarding their observance of AML/CFT/PF requirements; there have not been cases of non-observance. In 2015 and 2016, the Central Bank actively promoted the implementation of an automated TFS application system at all supervised entities — through forwarding clarifications, enhancing requirements towards ICR and relevant inspections on the execution of all the said. Currently, all FIs under the Central Bank's control use specialised software allowing for the automated search of enlisted persons.

798. Among all FI categories, there have not been cases of TFS application procedures non-observance, partially because of the inspection moratorium (except for FIs under the Central Bank supervision and unscheduled audits) in place for 2 years from April 1, 2018. Accordingly, sanctions have not been applied and there have not been presented selected statistics. Herewith, private sector representatives have demonstrated examples of TF TFS application (see IO.10) which implementation mechanisms being identical to TFS relating to PF, as well as the examples of "false positive". It should be noted that with the adoption of PCM-402 in June 2021, supervisors were able to monitor and control with a risk-based approach, which in the future, will improve the effectiveness of control in the DNFBP sectors (see IO.4).

799. Sanctions for AML/CFT requirements non-observance towards DNFBP are not applied in practice, including due to the moratorium mentioned, thus, their restricting function is impossible to evaluate.

800. Central Bank follows a comprehensive approach to constant training of supervised bodies' staff. For the rest of FIs AML/CFT/PF training (including TFS-related) has been regularly held by FIU, supervisory bodies, Association of Leasing, and commodity exchanges. All DNFBP are regularly trained on TFS issues by supervisory bodies and DCEC. The sectors are on a recurring basis being forwarded to methodological recommendations on TFS application, however, it should be noted that there has not been developed any special guidance on PF and related typologies.

801. There have regularly been conducted the Republic of Uzbekistan General Prosecutor's Academy-based round table discussions, workshops and other educational events with the participation of law

enforcement and supervisory bodies as well as private sector representatives — PF TFS issues being among other ones.

802. Besides, the majority of reporting entities while meetings with assessors have admitted that they regularly refer to DCEC and receive clarifications on legal requirements and practical application of TFS for PF.

Overall conclusions on IO.11

803. Taking into account that the Republic of Uzbekistan has taken practical measures for immediate enlisting of PF involved persons, communicating the List to reporting entities and for assets freezing, the country has demonstrated a significant level of effectiveness. Assessors have admitted the necessity for moderate improvements relating to the adoption of clearly set penalties for individuals and legal entities (that are not either FIs or DNFBP) who do not stick to PF TFS requirements, development of more detailed guidance for the private sector on the practical implementation of PF TFS requirements, as well as improving abilities of reporting entities regarding the identification of the companies owned or controlled by those PF enlisted.

804. **The Republic of Uzbekistan is rated as having a substantial level of effectiveness for IO.11.**

CHAPTER 5. PREVENTIVE MEASURES

Key Findings and Recommended Actions

Key findings

Financial Institutions

1. FIs demonstrated an understanding of ML/TF risks (strong understanding: banks, payment organizations, NBCIs, leasing companies; adequate understanding of risks, and full understanding of vulnerabilities: commodity exchange members, postal operator; limited understanding: professional securities market participants, insurance companies) based on the NRA findings and training activities conducted by the competent authorities. All FIs understand their AML/CFT obligations. Certain categories of FIs conducting commercial activities or transactions listed in the FATF glossary are not included in the AML/CFT system. However, the level of this deficiency is minor, as only certain types of FIs are exempted from regulated sectors (rather than the whole sector).
2. Risk mitigation measures, including by addressing the identified vulnerabilities, among FIs are equally well applied by banks, commodity exchange members, payment organizations, NBCIs and the postal operator. The other representatives apply mitigation measures to a satisfactory extent.
3. FIs effectively apply CDD measures, identify customers' BOs, monitor customers' transactions, and keep obtained data. There are cases when customers are denied services when it is impossible to complete CDD procedures in banks, stock exchange trading sector, NBCIs and leasing organisations. The remaining FIs have no cases and no statistics on refusals when it is impossible to complete CDD procedures, but this shortcoming is assessed to be moderate given the weight of the sectors.
4. FIs adequately apply enhanced CDD measures for foreign and international PEPs, while they are not applied for domestic PEPs, due to the lack of such requirement in the legislation, which negatively affects the AML/CFT system. Banks and payment organizations effectively assess ML/TF risks of new products and technologies before they are introduced into the market, but other FIs do not comply with this requirement due to insufficient awareness of it. FIs understand and apply their TFS obligations in substantial level. FIs successfully apply enhanced CDD measures in respect of correspondent banking relationships, electronic money transfer, customers from higher risk countries as defined by the FATF, while certain banks – in accordance with their internal policies – refuse to on-board such customers.
5. Banks, exchange members, professional securities market participants, NBCIs and payment organizations in substantial level perform an STR filing obligation in accordance with the established criteria of suspicion and not to inform customers about it. Other financial institutions implement requirement on STR filing in practice to a lesser extent.
6. All FIs have a well-constructed AML/CFT internal control system. Insurance companies, due to limited understanding of AML/CFT risks, do not appoint a separate AML/CFT officer, but instead assign AML/CFT internal control responsibilities to existing employees. Banks and the postal operator are good at assessing the effectiveness of their AML/CFT internal controls internally. In other sectors, only large FIs perform non-mandatory audits of the AML/CFT system, with internal controls being carried out by FI executive body.

DNFBPs

7. The understanding of AML/CFT risks and responsibilities varies across DNFBP sectors. Lawyers, notaries and auditors demonstrated a significant understanding of such responsibilities, as well as of ML/TF risks. The notaries' sector is also the only one that has demonstrated a substantial understanding of risks, backed up by the application of enhanced CDD measures and filing STRs. The real estate agents sector also showed a substantial understanding of the risks and knowledge of its obligations. The DPMS sector, having the highest risk level, by contrast, is characterised by

a moderate understanding of AML/CFT obligations and a low level of implementation of preventive measures in practice.

8. All DNFBPs apply measures to mitigate ML/TF risks while onboarding customers and checking them against TF/PF lists.
9. Some DNFBP sectors (notaries, lawyers, auditors) have demonstrated a substantial understanding of their CDD obligations, while the DPMS sector, for example, limits itself to the identification of the customer at the onboarding stage. Nevertheless, all DNFBPs indicate that it is not possible to serve a client without identification; if it is impossible to carry out CDD, the client will be refused service. All DNFBPs present in Uzbekistan understand the obligations of record keeping for a period of five (5) years after the termination of the relationship with the client and fully comply with this obligation.
10. Examples of the application of enhanced CDD measures among all DNFBPs are demonstrated only by notaries and lawyers. Issues related to the risks and specific features of servicing PEPs are understood at a substantial level in the sector of lawyers and notaries. In other sectors, this understanding is at a moderate level. All DNFBPs demonstrated their understanding of the need to conduct ML/TF risk assessments of new products and technologies before using them but did not demonstrate any examples for there were none. All DNFBPs understand their TFS obligations.
11. Despite the fact that all DNFBPs understand their obligations pertaining to the provision of information to the authorised body, not all sectors file STRs and provide other material information, except for the sector of notaries who sent 4 STRs over the reporting period. Besides, the limited understanding of this obligation was demonstrated by the DPMS sector.
12. Although all DNFBPs develop internal documents for the purposes of complying with AML/CFT requirements and appoint officials responsible for compliance with the ICRs, most DNFBPs appear to adopt a perfunctory approach to complying with AML/CFT requirements that consists of the non-identification of ML/TF risks and, as a result, the absence of STRs and other material information.

Recommended actions

Financial institutions

1. Supervisory authorities should continue to work with FIs (securities and insurance sector) to improve their understanding of ML/TF risks. The methodology of risk assessments for FIs that have demonstrated an incomplete understanding (exchange members, the postal operator) should be clarified.
2. Commodity exchanges, the central depository, the stock exchange and mobile operators involved in money transfers, should be included in the category of reporting entities. It should be clarified in legislation that reporting entities do not include all postal service providers, but only those who conduct money transfers.
3. Risk mitigation plans should be developed and implemented following internal risk assessments at FIs (except for banks and the postal operator).
4. Due to a large number of high-risk customers at FIs, in order to improve the quality of risk management, supervisors should optimize the approach to establishing mandatory criteria for high-risk customers and transactions for the purpose of applying enhanced CDD measures.
5. Risks of new technologies and products should be assessed (except for banks and payment organizations).
6. STRs should be filed when CDD procedures cannot be completed (except for banks, the stock exchange sector, NBCIs, and leasing organisations). Insurance organizations, the postal operator and leasing organizations should improve the understanding of the STR filing obligation. FIs should be guided in filing STRs based on the suspiciousness of transactions rather than threshold criteria (except for banks). The FIU should develop codes for dubious transactions based on the typologies identified instead of the single «999» code used.

7. Insurance companies, leasing companies and professional securities market participants should automatize their systems so that persons from their customer base can be checked against the List.
8. Audits and/or internal control over the inspection of the AML/CFT system should be carried out by FIs (except for banks and the postal operator).
9. Increase the level of compliance with requirements relating to the application of enhanced CDD measures, in particular in relation to PEPs and their family members or close associates.

DNFBPs

10. Strengthen understanding of ML/TF risks and ensure proper implementation of AML/CFT obligations by those DNFBP sectors that have limited understanding of risks and responsibilities, paying specific attention to the DPMS sector as it is most vulnerable to ML/TF risks.
11. Increase the level of compliance with requirements relating to the application of enhanced CDD measures, in particular in relation to PEPs and their family members or close associates.
12. It should be considered whether it is possible to optimise the indicators of suspicious activity established in the ICR for different DNFBP categories with due regard to the specific features of business and recent typologies.
13. Conduct a risk assessment of independent legal professionals (not lawyers) and organizations providing accountancy servicses and, based on the results of the assessment, decide whether they should be included in the AML/CFT/CPF system as entities providing services in accordance with the Recommendation 22.
14. Cooperation should be organized between the FIU and the supervisory authorities in relation to the scope and quality of the information received from DNFBP sectors, and develop and implement a set of measures aimed at identifying the reasons for the lack of STRs and other relevant information from the sector and eliminate them.

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

Immediate Outcome 4 (Preventive Measures)

806. The analysis and conclusion on IO.4 are based on meetings with the private sector (the assessors met representatives of all categories of FIs and DNFBPs), available examples and statistics, and information received from the supervisory authorities.

807. The assessors did not evaluate measures taken by the VASP since the only exchange in the country was not actually operating at the time of the on-site visit.

808. In assessing the effectiveness of IO.4, the assessors considered the volume of assets and transactions, as well as the characteristics of various FI and DNFBP categories to determine their relative weight in the overall picture.

FI sector

809. When assessing the results of preventive measures under Immediate Outcome 4, the main weight was given to the banking sector as the most significant one, through which the vast majority of financial flows of both legal entities and individuals pass and which is also more exposed to ML/TF risks.

810. Commodity exchange members were identified as the second most important category of FIs based on transaction volume. However, the ML/TF risks in the sector are insignificant, as they are mitigated due to the fact that all transactions are conducted through banks.

811. The sector of payment organizations is defined as the third most important based on transaction volume, but ML risks are assessed as moderately high (TF risks are low).

812. The weight of other categories of FIs was considered by the assessors to be insignificant due to the insignificant proportion of their transactions and the scope of services they offer in the context of the financial system of Uzbekistan.

DNFBP sector

813. The assessors paid increased attention to the analysis of the activities of DPMS, notaries, lawyers, and real estate agents as these sectors are important among all DNFBP categories, and less attention to the activities of lotteries and accounting firms. The importance of DNFBP categories was determined based on the number of registered participants in each category and the identified ML/TF risks. Chapter 1 provides a more detailed justification for the weighting of the DNFBP sectors.

814. The assessment revealed that independent legal professionals and accounting services organizations provide company creation services in the country. However, they are not covered by the AML/CFT legislation.

Understanding of ML/TF risks and AML/CFT obligations

815. All FIs and DNFBPs demonstrated an understanding of ML/TF risks and their AML/CFT obligations. The level of understanding varies depending on the size of the sector. From among FIs, banks, the payment sector, NBCIs and leasing organizations demonstrated the best understanding; an uncomplete understanding of risks, but full understanding of vulnerabilities was demonstrated by exchange members and the postal operator. Of all DNFBPs, auditors, lawyers, and notaries showed a substantial level of understanding of ML/TF risks and their obligations in this area. The other DNFBPs to a lesser extent.

Financial institutions

816. All FIs demonstrated a general understanding of ML/TF risks and risk management measures based on NRA findings (all of them took part in the NRA) and training events organised by the competent authorities. The NRA and sectoral risk assessments (SRA) were conducted between 2018 and 2021 in all sectors (except for the stock trading sector involved in the NRA). All FIs demonstrated knowledge of the full range of their AML/CFT obligations.

817. Banks, payment organizations, the postal operator, NBCIs (microcredit organisations and pawnshops) demonstrated examples of documented internal risk assessments. The responsible persons of exchange members annually prepare activity reports and submit them to the FIU.

818. Banks demonstrated awareness about the results of the NRA and SRA, which shows their understanding of the risks set out in these documents and is assessed positively by the assessors. According to documented bank risk assessments, the following ML/TF risks have been identified in banks: a) withdrawal by individuals of cash foreign currency from bank cards issued by foreign banks through ATMs; b) lending operations, mainly related to preferential lending; c) depositing cash foreign currency in the settlement accounts of business entities as proceeds from export contracts, by proxy on behalf of non-residents; d) operations of legal entities carried out through remote banking systems (Internet banking), e) online purchases using international bank cards.

819. Based on the ICR, the risk assessment methodology developed by the Central Bank and their own methods, banks annually identify and assess the ML/TF risks of banks in the following areas: a) customers' risks: non-residents, non-profit non-governmental organisations (NGOs), customers with a complex ownership structure, customers engaged in suspicious transactions in a regular basis, trade, services, construction, agriculture; b) risks of products and services: online credits, international bank cards, trade financing, currency trading; c) risks of the sales channels of products and services (technology risks): remote banking services, payments via mobile applications, ATMs; d) geographic risks (features of geographic "presence"): FATF lists, offshore areas, areas of increased terrorist activity, sanctioned countries, countries with a high level of corruption and crime.

820. The stock trading sector completely understands the ML/TF vulnerabilities. Representatives of the sector consider ML/TF risks insignificant, as they are mitigated due to the fact that all transactions are conducted through banks. However, it should be noted that banks define the ML/TF risk coming from violations of trading or service provision rules as high (in accordance with the NRA).

821. Payment organisations identify the risk of fraud and ML threat via P2P transactions (money transfers via mobile banking applications between two parties with the use of debit, credit cards or individual

bank accounts) between individuals, including a) activities without state registration; b) activities without a licence, including illegal payment service activities; c) fraud. The understanding of risks in this sector is assessed as good.

822. The postal communication operator has a good understanding of its place in the financial sector and the conditions of its activities in order to assess the current and potential ML/TF risks. Representatives of the sector have shown an understanding of the main vulnerabilities. In this regard, it may be noted that representatives of the sector do not completely understand the difference between vulnerabilities and risks.

823. As noted, the other sectors are also well aware of the risks identified in the NRA and SRA. However, there are the following deficiencies: the securities sector lacks an understanding of the risks posed by remote services, insurance companies are not aware of ML typologies through life insurance schemes. The understanding of ML/TF risks by these sectors is assessed as satisfactory. Leasing companies identified the absence of a supervisory authority as their main vulnerability in the SRA, yet the sector is well aware of the risks inherent in leasing services.

824. All FIs have demonstrated a good understanding of their obligations and comply with them adequately. Financial institutions are especially well aware of the obligations to conduct customer due diligence, enhanced due diligince and STRs filing.

VASPs

825. The only licenced VASP UzNEX approved the internal cryptocurrency exchange trade regulations that feature a separate chapter on measures to be taken to ensure compliance with the AML/CFT laws, where the exchange identifies its risks and AML/CFT obligations. It was not possible to assess the effectiveness of these efforts at the time of the on-site visit since the VASP actually did not operate.

DNFBPs

826. DNFBPs were actively involved in the ML/TF NRA. To this end, the supervisory authorities sent them questionnaires to be filled in. In 2018, SRAs were conducted in the sector of notaries, lawyers, and auditors. A similar assessment was conducted in respect of DPMSs in 2020. The SRA and NRA findings were brought to the notice of organisations via the supervisory authorities. It should be noted that representatives of the sectors where SRAs were conducted demonstrated a deeper understanding of not only risks but also their obligations to mitigate them.

827. Representatives of the DPMS sector demonstrated a moderate understanding of ML/TF risks, mainly focusing their attention on the threats of stolen precious metal wares being sold. Overall, agreeing with the findings of the ML/TF NRA and SRA, representatives of the sector have demonstrated a moderate understanding of their obligations, which are limited to basic CDD and TFS procedures in relation to persons involved in TF/PF. AML/CFT reports, including risk reports, are not sent to the supervisory authority. Representatives of the sector did not demonstrate their knowledge of ML/TF typologies or understanding of the vulnerabilities of the sector in terms of money laundering.

828. In the context of Uzbekistan, it is important to note that the DPMS sector is characterized by small volumes of transactions, the vast majority of representatives of the sector are small businesses and individual entrepreneurs, which implies a low probability of using the sector in money laundering schemes characterized by significant amounts.

829. Notaries and lawyers also have a good understanding of ML/TF risks and substantially fulfil their AML/CFT obligations. Both lawyers and notaries were involved in the preparation of the ML/TF NRA and annually send risk reports to the supervisory authority in accordance with their obligations set forth in the ICR. Lawyers are better aware than notaries of obligations to take measures to identify PEPs from among their customers and the BOs of customers in order to mitigate risks associated with corruption and the management of companies by criminals, though there were no examples of how PEPs were identified in practice and what measures were taken.

830. Representatives of the real estate sector generally demonstrated a substantial level of understanding of ML risks and annually send risk reports to the supervisory authority. The understanding of risks in

the sector is still rather theoretical in nature, which stems from the knowledge of NRA findings and obligations set forth in the ICR. Real estate agents in Uzbekistan are substantially aware of their AML/CFT obligations, but due to the fact that real estate agents in Uzbekistan cannot engage in real estate transactions on behalf and for their clients and confine themselves to the provision of intermediary and consulting services, cases, where it is necessary to apply enhanced CDD measures in addition to standard CDD, deny services or refuse to conduct a transaction, are extremely rare.

831. Representatives of the audit sector demonstrated a good understanding of ML/TF risks and their responsibilities in this area. First and foremost, this applies to their CDD and customer risk assessment obligations. All auditors assess the risks of their customers, taking into account the conducted NRA and SRA. The high level of understanding of risks and obligations is also facilitated by annual obligatory training of auditors in order to improve their skills.

Application of risk mitigating measures

832. Risk mitigation measures are evenly well applied by banks, microcredit organisations, the postal operator, exchange members and payment organisations. The rest of the FI - to a satisfactory degree. The assessors believe that all DNFBPs can fully perform their obligations to mitigate ML/TF risks. However, DNFBPs sectors demonstrate a diverse understanding of such obligations.

Financial institutions

833. FIs have established internal controls and systems to mitigate risks. All banks and payment organizations, as well as in VASPs have compliance departments that efficiently operate and organise AML/CFT activities. AML/CFT matters are resolved at the level of heads of banks and supervisory boards.

834. To obtain access to stock trading, all traders of exchange members undergo testing and interviews pertaining to AML/CFT and internal control organisation. Two (2) designated persons are appointed by order at every commodities exchange. Each exchange member is ordered to appoint a designated person responsible for compliance with the ICR. These measures are assessed by experts as adequate for risk mitigation.

835. The other FIs usually appoint designated persons responsible for the implementation of the ICR. Insurance companies, due to their weaker understanding of AML/CFT risks, do not appoint a separate AML/CFT officer, but instead assign AML/CFT internal control responsibilities to existing employees (these are generally the Deputy Head of the company, the Head of the Risk Management Department, the Head of Security or Legal Counsel), which negatively affects insurance companies' compliance with their AML/CFT obligations.

836. Banks took mitigating measures in relation to risks mentioned in c.i. 4.1: cameras were installed, threshold amounts were set for ATMs; card and credit limits were introduced; cash declarations are inspected, transactions are controlled and monitored; customer service agreements are suspended and terminated. These measures are assessed by the assessors as effective, proportionate and adequate. It is worth noting that there are a large number of customers served by banks in relation to whom enhanced CDD measures are applied. For instance, in terms of customers who underwent enhanced CDD procedures in 2019, 25.5% were legal entities, 45% – were individual entrepreneurs, and 6.6% – were individuals. This is an obligatory requirement (to apply enhanced CDD measures) for customers with a high level of risk and a low level of risk who conducted a high-risk transaction. Moreover, high risk is automatically assigned to both customers and transactions based on the criteria established by the supervisory authority, which is not conducive to the effective management of risks. Similar criteria-based controls are set for the customers of microcredit organisations and pawnshops. No statistics on high-risk customers and/or transactions were provided for other FIs.

837. The stock trading sector's supervisory authority developed and approved a plan of practical measures to be taken to mitigate AML/CFT risks in the stock trading of commodity exchanges and their members. Deficiencies in the ICR were addressed and sanctions were revised as planned. The assessors evaluated these efforts in IO 3. ML/TF risk assessment forms (in relation to customers and

transactions, following which statutory measures are applied) were developed and put into practice for exchange members. Moreover, based on the typologies of fictitious sale operations identified in the stock trading sector, measures were taken for enhancing control over such transactions and filing STRs.

838. To reduce the risk of fraud, payment organisations, on discovering that an account was accessed from a different device, send an SMS to the number assigned to the account. Users regularly receive notifications, also news is published on the company's website and social media. Effective measures are in place: there is a register of stop lists of bank cards and electronic wallets, control over IP addresses by location, monitoring, and payment limits. These measures correlate with the risks identified in the sector.

839. Following the NRA, microcredit organisations created a special in-house monitoring department in order to inspect directly the customer's activities by making on-site visits. Pawnshops have video surveillance and twenty-four-hour security in order to mitigate all potential risks. Pawnshops and microcredit organisations always properly verify the source of funds and monitor that funds are spent in accordance with their intended purpose. In particular, they request information from customers in questionnaires, make on-site visits and verify the existence of facilities for which a credit is granted (e.g., construction of cold frames and so on).

840. Representatives of the sector of postal money transfers noted at the meetings that they took the following measures to mitigate risks: a) they developed and introduced changes and additions to the ICR; b) they introduced a new automated postal money transfer system; c) they approved a note on the user due diligence and introduced a mechanism for the identification of foreign PEPs; d) they prepared and distributed among employees of Uzbekiston Pochtasi JSC learning materials, slides and videos. This helped mitigate the vulnerabilities identified during the risk assessment.

841. In the securities sector, the central depository is introducing (did not yet introduce at the time of the on-site visit) software that makes it possible to automatise customer monitoring and securities transaction processes.

842. To address a number of deficiencies identified in the SRA, changes and additions were introduced into the ICR for insurers and insurance brokers (registration No. 2036-3 of 26 June 2021 with the Ministry of Justice).

843. All FIs train their employees in the AML/CFT area as one of the risk mitigation measures.

DNFBPs

844. The assessors believe that all DNFBPs have all opportunities and resources, including information provided by the supervisory authorities, to understand ML/TF risks in their areas of activity, and have a complete opportunity to perform their obligations with a view to mitigating ML/TF risks in accordance with the nature of their activities.

845. The understanding of risk mitigation measures in most DNFBP sectors is at a moderate level. All DNFBPs take action to mitigate ML/TF risks mostly when on-boarding customers and checking them against the Lists of Terrorists. For this purpose, all DNFBPs sectors are connected to the personal account on the website of the FIU where they can familiarise themselves with the above Lists. Other DNFBPs sectors do not regularly assess the risks of customers, but representatives of all sectors demonstrated an understanding of geographic risks and risks associated with dubious transactions.

846. Moreover, to cooperate with the supervisory authorities, online specialised software platforms such as "Valuation and Real Estate Activity", "Notary" automated information system, and PC "Audit" are in place, but these resources were also used to transfer information about updates to the Lists at the time of the on-site visit. At the same time, to reduce the risk of providing services to customers with a bad business reputation, auditors, lawyers, notaries, and real estate agents use publicly available sources, including commercial databases. However, it is impossible to assess the effectiveness of such work since there are no examples of similar efforts, and DNFBPs (except for four STRs filed by notaries) almost never provide STRs and other information such as in cases when the customer is

denied services. All sectors note that it is possible to cooperate with LEAs when one identifies criminals in persons who requested services, but there are no examples of such efforts either.

847. According to the SRA, 90% of the DPMS sector are small and micro enterprises that may be exposed to the risk of involvement in ML/TF schemes. Individual entrepreneurs can independently stamp and sell jewellery which creates a major vulnerability that makes it possible to exploit the sector for the legalisation of criminal jewellery. As representatives of the DPMS sector refer to the possibility of taking a stolen piece of jewellery on commission as the principal threat, the main procedures relating to the establishment of business relationships particularly concern the mitigation of the risk of a knowingly stolen piece of jewellery being sold when taking it on commission. Accordingly, there are in fact no AML/CFT risk mitigation measures when it comes to selling jewellery (i.e., in relation to buyers).

848. Real estate agents generally understand the risks associated with serving customers in certain categories (e.g. PEPs, designated persons) and geographical risks. Real estate agents are not obliged to participate in real estate transactions, which, in their opinion, contributes to the absence of persons possibly involved in ML/TF among their customers. The risks of involvement of the sector in ML/TF are also minimal due to the mandatory notarization of real estate transactions between individuals.

849. As in the case of notaries, real estate agents' understanding of their AML/CFT obligations is generally satisfactory, although there is a lack of understanding of the obligations related to the establishment of BOs in relation to individuals. Due to these features of the system, real estate agents position themselves more as consultants, rather than intermediaries and do not pay sufficient attention not only to the customer but also to the source of funds, indicating that this issue is beyond their competence. In connection with the above due to the lack of practice in applying enhanced CDD measures, refusing to provide services to customers and filing STRs by real estate agents, it is not possible to assess the effectiveness of risk mitigation efforts.

850. In order to comply with the requirements of the PCC and for the purpose of mitigating ML/TF/PF risks, each audit organization develops internal rules for ML/TF risk mitigation purposes. These rules apply to professional accounting services that are not provided by the representatives who took part in the meeting with the assessors. The head of each accounting firm issues an order of appointment of at least one designated person responsible for internal controls and compliance with the ICR.

851. All designated persons are staff auditors of the company for whom this organisation is the principal place of employment. Given the specific aspects of activities, of working under international standards and with corporate customers, auditors completely understand their BO identification obligations and generally pursue the Know Your Customer policy.

Application of CDD and record-keeping requirements

852. FIs effectively apply CDD measures, monitor transactions, and keep obtained data. When identifying BOs, FIs rely on data obtained from the customer, as well as from publicly available sources. When it is impossible to complete CDD procedures, FIs refuse business relationships with their customers.

853. However, DNFBP sectors demonstrate a diverse understanding of such obligations. All DNFBPs deny services if they have suspicions that the customer’s purpose is ML/TF or when they cannot conduct CDD. Not all DNFBPs identify and can identify BOs (except for notaries, lawyers, and auditors). All DNFBPs represented in Uzbekistan understand their obligation to keep data and information for five (5) years after terminating their relationships with the customer and fully perform this obligation.

Financial institutions

854. Identification of a customer that is an individual is carried out on the basis of a document (passport or another document) proving his/her identity, or biometric data. In this case, the employee of the FI verifies such data with the information system of the Ministry of Internal Affairs, which is sufficient for the purposes of CDD of residents of the Republic of Uzbekistan.

855. When applying CDD measures to legal entities and individual entrepreneurs, an employee of the FI shall obtain from them: a) state registration documents; b) information on the heads and details of constituent documents. The information is verified through the automated system of state registration and registration of business entities.

856. Identification of customers' BOs in the CDD framework is performed by FIs using the information provided by the customer itself and documented, which is effective. Besides, state and commercial databases and other public sources are used for data verification and additional research. Such databases and sources include a) websites of the SSRBE[61], SSREO[62], websites where data on trademarks is presented[63]; b) open data channels on the Internet, social networks and official websites of companies; c) open sources of other states (in the case of verification of non-resident customer data and identifying BOs of non-resident customers)[64]. If, as a result of the measures taken, doubts arise as to whether the person with the controlling interest is a BO, the bank may confirm or deny this information by analyzing the customer's banking transactions. FIs confirmed that they can provide data on their customers' BOs at the written request of the regulator (Central Bank, FIU). Where the ownership structure of the customer that is a legal entity is complex, the FI examines the ownership structure of each legal entity involved in the chain and moves "in-depth" to the identification of specific individuals, which is considered by assessors as effective work.

857. All customer data are entered into questionnaires. In the FIs controlled by the Central Bank, this process is automated and questionnaires are kept electronically. The customer questionnaire shall be kept by the organization for at least 5 (five) years from the date of termination of the relationship with the customer. As the information indicated in the questionnaire changes, as well as the nature of the financial transactions conducted by the customer, the FIs shall reconsider the risk level of working with that customer. To verify the data, requests are sent to state authorities (statistics and examples of requests are provided). In case of high risk, customer information is updated at least once a year, in case of low risk – once every two (2) years. The assessors consider these measures to be sufficiently effective.

858. In the banking sector, there are cases of refusal to provide services to customers due to the inability to complete CDD procedures followed by filing STRs. It should be noted that NBCIs and payment organizations had cases of refusal to provide services to customers due to inability to complete CDD procedures, but such situations were not recorded by the above organizations (some NBCIs began to record such cases starting in 2020).

859. Banks showed examples of refusals to on-board due to negative information about the customer, impossibility to identify the customer's BO, as well as refusals due to doubts about the authenticity of documents.

Table 4.1. Information about banks denying transactions for 2016–2020

Year	Number of banks	Refusal to enter into business relationships	Refusal of a transaction	Termination of business relationships	RB services were disabled
2016	2		1		4
2017	4		2	2	3
2018	4		2	1	5
2019	8	5	12	3	7
2020	11	67	344	359	418
Total 1,235 cases		72	361	365	437

860. According to the 2019 SRA relating to the banking sector, that there were no provisions in the AML/CFT Law made it difficult to refuse transactions when it was impossible to apply enhanced CDD measures set forth in the ICR. Banks preferred to file a report about a suspicious transaction to

[61] https://fo.birdarcha.uz/pub/search
[62] http://registr.stat.uz/enter_form/ru/index.php
[63] www.openinfo.uz
[64] https://find-and-update.company-information.service.gov.uk/; https://efiling.drcor.mcit.gov.cy/DrcorPublic/; www.icris.cr.gov.hk

the FIU rather than exercise their right of refusal. As a consequence, the Central Bank jointly with the DCEC took relevant measures, in particular introduced changes and additions to paragraph 24 of ICR No. 2886 of 23 May 2017. As of 2020, banks have actively started implementing this paragraph in practice, which accounts for a fairly high number of refusals over this period.

861. Banks and NBCIs commit a large number of violations (thousands) of the procedure for surveying customers, but this is mainly due to the transfer of databases to new software systems and technical failures, as well as operational errors of personnel. Similar reasons served to reveal a large number of questionnaires for which the banks failed to provide storage for the prescribed period (5 years).

862. Representatives of the stock trading sector fully understand and apply the CDD measures, including the BO identification, data updating and keeping. There are isolated cases of violations of CDD requirements related to the failure to keep constituent documents of the exchange member's customers. At the same time, there are cases of refusal to conduct a customer's transaction if the information required for CDD is not provided.

863. Operators of payment systems, electronic money systems and payment organizations, payment agents (subagents) trust the results of CDD conducted by banks. In this case, all legal requirements regarding the reliance on third-party measures are satisfied.

864. The other FIs understand and apply CDD measures, conduct the BO identification and keep data at a moderate level. For example, in the insurance sector, the BO identification measures are generally limited to verification of data on the customer itself, because in practice there are no cases where a legal entity is indicated as the beneficiary. There are no cases and statistics of refusals on the grounds of inability to complete CDD procedures (except for banks, the stock trading sector, NBCIs and leasing organizations). However, considering the materiality of the sectors, the above deficiencies are assessed as moderate.

865. The ongoing monitoring and verification of customer transactions are carried out by the staff of the FIs directly serving customers (responsible executors, cashiers, etc.) according to their job descriptions, who, when they identify a suspicious transaction that meets the established criteria, report such transactions to their direct supervisor, a responsible officer or the Internal Control Service. Such work is carried out with varying degrees of success by multiple FIs.

866. The follow-up inspection of customer transactions shall be carried out by a responsible employee or by the Internal Control Service by analyzing customer transactions conducted during the previous period in order to identify suspicious transactions not identified at the stage of the current check.

867. FIs controlled by the CB (banks, payment institutions, NBCIs), as well as professional participants in the securities market effectively use software products to automatise the process of identifying suspicious transactions according to developed and predetermined criteria.

VASPs

868. According to the Rules of crypto-exchange trading, VASP UzNEX has introduced a mechanism of mandatory identification of users, carried out regardless of the transaction amount. In case of refusal to undergo the identification procedure, the user is not allowed to trade. According to the Rules, the VASP provides keeping of data on transactions and customer interactions for 5 (five) years. At the time of the on-site visit, the only licensed VASP didn't work, so there are no statistics of refusals to establish business relations or conduct transactions.

DNFBPs

869. DPMS conduct CDD in all cases involving the turnover of precious metals and precious stones, including when it comes to establishing business relationships (in accordance with the approved ICR). This is necessarily done in light of the sector's risk associated with the fact that stolen pieces can be taken on commission. An exception to this is a sale (i.e. a one-time deal) during which CDD is conducted when the price exceeds ~ USD 7,000. However, according to representatives of the sector, CDD is still limited to the identification of the customer's identity, which indicates that these measures are insufficiently effective.

870. Representatives of the DPMS sector did not conduct one-time transactions selling jewellery exceeding the threshold amount, in view of which no CDD was conducted in such cases. Based on available information, the assessors are inclined to believe that, when a piece is taken on commission for further resale, no CDD is conducted for AML/CFT purposes, and identification is performed to the extent necessary to take the piece on commission in accordance with industry-specific laws. The interviewed representatives of the sector stated that they did not face the need to take enhanced CDD in practice. Information provided by the customer is not verified either. With that said, the understanding of AML/CFT obligations, including insofar as CDD and features of these customer servicing procedures are concerned, is low in the sector and does not make it possible to properly mitigate the risks of involvement in ML/TF schemes.

871. Notaries and lawyers apply standard CDD procedures in all cases and identify BOs. Representatives of the sector of lawyers' services largely understand this obligation, whereas notaries conduct CDD only when this concerns the customer that is a legal person. Notaries and lawyers verify information provided by the customer that is a legal person. To do so, notary offices use software capacities of the "Notary" automated information system, whereas lawyers use publicly available sources.

872. Both notary offices and lawyers' associations appoint a designated employee responsible for AML/CFT who determines the level of customer risk based on transactions they conduct and the information they provide. Notary offices and lawyers' associations, as well as auditors, develop internal rules that establish a procedure for acting to identify, assess, monitor, manage, mitigate, and document risks. Based on this assessment, notaries periodically refuse to take notarial action. Refusals are made in accordance with Article 38 of the Law of the Republic of Uzbekistan "On the Notariat" and are not related to AML/CFT. Such refusals are recorded on a non-regular basis. As for lawyers who also report refusals to provide services in view of customers' risks, refusals are not recorded. As refusals are not recorded and there are no refusal reports (this obligation is not enshrined in the ICR of notaries and the ICR of lawyers; it is enshrined in the ICR of auditors but not applied), it is impossible to assess the efficiency of the above measures.

873. Real estate agents conduct CDD at the stage of establishing business relationships with buyers and sellers. Representatives of the sector report RBA elements insofar as customer servicing is concerned, by both territoriality (e.g., the customer comes from a different region) and the nature of the transaction (expensive real estate). The interviewed representatives of the sector report that such efforts are taken but mostly in the context of real estate risk assessment rather than in terms of ML/TF risk assessment. In the case of expensive real estate, the real estate unit and customer undergo additional inspections, which broadly evidences that certain restrictive measures are taken to prevent the real estate from being used in ML schemes.

874. When onboarding customers, audit firms do not put into practice such special AML/CFT measures as enhanced CDD, refusal to provide services to customers when there is an ML/TF risk and reporting information to the authorised body. However, auditors comprehensively assess the customer and identify BOs, check them against the Lists, verify information provided by the customer against publicly available sources. Such efforts are taken in order to assess the audit risk.

875. All DNFBPs represented in Uzbekistan understand their obligation to keep data and information for five (5) years after terminating their relationships with the customer and fully perform this obligation.

Application of EDD measures

876. Most FIs represented in the Republic of Uzbekistan effectively apply EDD measures. All FIs identify domestic and foreign PEPs at a similarly good level. When establishing correspondent banking relationships, banks exchange extended questionnaires with foreign banks, requests for suspicious financial transactions of customers' counterparties, and take other range of measures in order to identify their correspondent bank. Banks and payment organisations assess the ML/TF risks of new products and technologies before introducing them to the market. Other FIs did not reveal their approaches to these assessments reasoning that there is no practice of using such a category of

products in their work. The assessments suggest that other FIs do not completely understand the need for such assessments. Banks, the postal operator, payment organisations, electronic money system operators, and payment system operators comply with obligations relating to electronic money transfers to a sufficient degree. All FIs understand their TFS obligations at a similarly good level. All FIs apply EDD measures in respect of customers from higher-risk countries. According to their internal policies, certain banks do not on-board such customers.

877. Examples of the application of enhanced CDD measures among all DNFBPs are demonstrated only by notaries and lawyers. Real estate agents do not identify on-boarded foreign PEPs and do not identify persons associated with higher-risk countries. The DPMS sector does not assess the customer risk in terms of AML/CFT and does not act to identify BOs and foreign PEPs. All DNFBPs demonstrated their understanding of the need to conduct ML/TF risk assessments of new products and technologies before using them but did not demonstrate any examples for there were none. All DNFBPs understand their TFS obligations.

Financial institutions

PEPs

878. Most FIs effectively apply EDD measures when establishing business relationships with foreign and international PEPs (hereinafter IPEPs). Clients are requested to inform about the sources of their funds and/or sources of their financial standing. This information is verified using open data sources. However, there are no statutory requirements, and no similar measures are applied in practice when it comes to on-boarding domestic PEPs.

879. The bank establishes business relationships with IPEPs only with the consent of the chairman of the management board of the bank or his/her authorised deputy. Such clients are high-risk ones, and EDD measures are taken in relation to them, with their transactions undergoing detailed monitoring, as demonstrated by the banks during the onsite visit. In 2016–2019, the banks onboarded a total of twenty-three (23) IPEPs.

880. When identifying the client's connection with IPEPs, exchange members apply EDD measures. In July 2018, the ICRs were amended to include the necessity to pay increased attention to IPEPs. Between 2016 and July 2018, no PEP identification measures were taken, and between July 2018 and 2019, commodities exchange members identified no IPEPs.

881. The activities of payment organisations and payment system operators have been regulated since 2020, and no AML/CFT requirements were applicable to them before that. Since 2020 there are no cases of detection of IPEPs by this sector due to the absence of such customers. Considering the fact that before 2020 the functions of payment organizations were mainly performed by banks (except for two payment organizations), this deficiency is assessed as moderate.

882. The other FIs, except insurance organizations, understand and fulfil the obligations to apply EDD measures in relation to IPEPs. Representatives of FIs noted that a resident individual may have links with IPEPs (i.e. a resident of Uzbekistan may be a relative of a foreign PEP or a close associates), which demonstrated an understanding of AML/CFT risks in this area of activity.

Correspondent banking relationships

883. When establishing correspondent banking relationships, banks of Uzbekistan open Nostro accounts in foreign banks, exchange extended questionnaires with foreign banks, request suspicious financial transactions of clients' counterparties. Available data suggests that there are no Loro accounts in foreign banks.

884. Before correspondent relationships, apart from identifying a non-resident bank, an Uzbek bank: a) collects additional information with a view to gaining a complete understanding of the nature of activities of the non-resident bank (information is taken from both publicly available sources (mass media and online publications) and using commercial databases in order to check the bank itself and private shareholders and heads); b) reaches conclusions on reputation and the quality of supervision in the non-resident bank based on publicly available information and assesses whether any

investigations relating to ML/TF breaches were initiated in respect of this bank; c) assesses AML/CFT measures adopted by the non-resident bank; d) ensures that the non-resident bank applies international AML/CFT standards. The assessors consider these measures to be effective.

885. For the purposes of CDD, between 2016 and 2020, Uzbek banks filed at least one thousand (1,000) requests for additional information about the client's counterparty to non-resident banks, and responses were received. This served as a basis for proceeding with transactions or refusing to conduct them and for filing an STR. Banks processed more than 4,000 requests from non-resident banks over the above period, and responses were received in relation to all the requests. The assessors believe that these figures constitute evidence of effective interaction with correspondent banks.

New technologies

886. Banks and payment organisations assess the AML/CFT risks of new products and technologies before introducing them into the market. Representatives of other FIs indicated their understanding of relevant risks but failed to demonstrate any approaches to assessing them for there was no such category of products. Representatives of the sectors explained that, between 2016 and 2020, no new types and methods of transactions involving money or assets were introduced. The assessors note that electronic client servicing technologies are also developing in these sectors, but the ML/TF risks of these technologies are not assessed.

887. In the banking sector, there are examples when the Compliance Service of a bank banned the introduction of new products in light of a high ML/TF risk. The assessors positively evaluate this approach and find it effective.

888. There are examples when the risks of new products and technologies were assessed in the sector of payment organisations and risk mitigation measures were developed that the company has to apply when using this product. These measures were recorded in a report approved by the General Director of the payment organisation.

889. The securities sector highlighted certain matters pertaining to the introduction of new technologies. For example, when an investment intermediary changes the client's personal data, another investment intermediary who also provides services to this client may not become aware of these changes. For this reason, electronic personal data is checked against the client's available documents during every transaction. This software product is not effective in practice and needs to be improved. The sector should also analyse online services provided to customers as they may increase ML/TF risks.

Money transfers

890. Banks, the postal operator, payment organisations, electronic money system operators, and payment system operators sufficiently comply with electronic money transfer requirements.

891. There are a few statutory exceptions for internal money transfers when no CDD is conducted and, accordingly, no data about the senders is submitted together with the transfer, which is inconsistent with the FATF Standards (R.16).

892. Meanwhile, postal communication operators send and receive full information about the sender and recipient during any transaction. All information is accompanied throughout the electronic transfer chain. Money transfers have no threshold amount, and CDD is conducted at any request of the client. Representatives of the sector have full information about conducted transactions which evidences their full compliance with the requirements.

Targeted financial sanctions

893. All FIs understand their TFS obligations. The list is available online in the personal accounts of FIs on the website of the FIU. It is provided via a secure channel with acknowledgement of receipt. When the client's data matches the List, assets are immediately frozen, and a report is submitted to the FIU (indicating the amount of the frozen assets).

894. FIs controlled by the CB (banks, payment institutions, NBCIs) use special software to automatically search for persons included in the List, which allows for the effective implementation of the TFS. For more details see IO10-11.

895. The exchange has a procedure for recording that the Lists were promptly sent out. The Republican Universal Agricultural Commodity Exchange and the Uzbek Republican Commodities Exchange established a practice according to which exchange members are obliged to familiarise themselves with the Lists via their personal accounts. There is a trilateral agreement setting out that the Lists should be delivered to exchange members within 1 hour and 15 minutes, which is assessed positively by the assessors.

896. Representatives of the securities market and the insurance sector apply TFS only in relation to new clients and financial transactions of existing clients. As there are no software developments, these sectors cannot constantly and promptly check their entire client base against the updated List. When conducting CDD and identifying the client's data, leasing organisations manually check the data of all participants of a leasing transaction against the List. It is therefore recommended that insurance companies, professional securities market participants and leasing companies automate systems to identify persons from the List among their client base.

Higher risk countries

897. FIs apply EDD measures in respect of clients from higher-risk countries as defined by FATF and file STRs relating to their transactions. Certain Banks – according to their internal policies – do not onboard such clients.

898. Clients of FIs that are nationals of FATF blacklisted and greylisted countries are automatically classified as high-risk clients. Banks have special reporting forms for ongoing monitoring of their transactions. These special electronic reports also trace bank transfers sent to and from FATF blacklisted and greylisted countries, and then this is reported to the FIU. In view of the large number of high-risk clients at FIs, supervisors should optimise the approach to establishing mandatory criteria for high-risk clients and transactions for enhanced CDD measures in order to improve the quality of risk management.

899. Since 2018, the FIU has informed FIs about the list of countries located in active combat zones or immediately bordering them or controlled by terrorist organisations. Changes were introduced into the ICR, according to which an STR is filed in relation to each payment, each transaction of a person crossing the border of these countries. This resulted in a significant increase in STRs related to common transactions of persons crossing the Turkish border with a view to purchasing goods for further resale in Uzbekistan and payments for such goods. Most FIs and the assessors negatively assessed these facts, which demonstrates the inefficiency of the approach to complete STRs in respect of transactions not related to FT.

DNFBPs

900. EDD is regulated by the existing ICR in all DNFBPs. EDD should be conducted when high-risk clients/transactions are identified, but no examples of such measures in practice were provided, which indicates that most sectors, with the exception of auditors and notaries, adopt a perfunctory approach to assessing the client risk.

901. The DPMS sector does not assess the client risk for AML/CFT purposes and does not take action to identify BOs and foreign PEPs. Representatives of the sector understand risks associated with higher-risk counties but do not find them to be relevant. Overall, according to the NRA, the sector is not involved in TF/PF, which confirms this conclusion of the representatives of the sector. There were no similar cases in practice.

902. Both notaries and lawyers understand the necessity to conduct EDD when one of the parties to the transaction is a person living, staying, or registered in a state that is not involved in international AML/CFT cooperation, or in an offshore zone. However, representatives of the sector did not provide any actual examples of such measures in practice.

903. Real estate agents do not identify on-boarded foreign PEPs and do not identify persons associated with higher-risk countries either. The provided information is not checked. In view of that, there are no recorded on-boarding refusals or refusals to conduct a transaction either.

904. Auditors examine their clients, not in order to comply with their AML/CFT obligations but rather to assess the audit risk, which is not indicative of the effectiveness of such measures.

905. All DNFBPs indicated their understanding of the necessity to assess the ML/TF risks of new products and technologies before using them but did not demonstrate any examples for there were none. The sectors of DPMS and real estate agents do not see any risks associated with new technologies for it was impossible to use them in their activities at the time of the onsite visit. It is possible to agree with this statement since the assessors do not have information about any new financial technologies being used in the above areas.

906. All DNFBPs understand their TFS obligations (for more information, see the analysis on IO.10 and IO.11). There were no cases of frozen funds at the time of the onsite visit. All DNFBPs examine only new clients for coincidence with the Lists. The assessors positively rate the efforts of DNFBPs in terms of applying TFS.

907. All DNFBP sectors are aware of the need to take special measures in relation to customers associated with states and territories identified in the official FATF statements, which pose a threat to the international financial system and have strategic deficiencies in their AML/CFT system.

908. After discussing CDD and EDD, it may be concluded that most DNFBPs have a limited understanding of these obligations. Only notaries and lawyers meet these requirements for AML/CFT purposes, whereas the DPMS sector and real estate agents did not provide any examples of EDD during the onsite visit.

Reporting obligations and tipping off

909. Of FIs, banks, exchange members, payment organizations, professional securities market participants and NBCI and pawnshops comply with their STR filing and tipping-off prohibition obligations equally well. Banks demonstrated that they perform a more proper analysis of transactions, including by developing their own dubious transaction criteria.

910. The FIU does not receive STRs and other material information from DNFBPs represented in Uzbekistan (except notaries who filed four (4) reports between 2016 and 2020).

Financial institutions

911. Banks, exchange members, payment organization sector, professional securities market participants, and NBCI (pawnshops, MCO) actively perform their STR filing obligations in accordance with the established criteria of suspiciousness. Microfinance organisations, the postal operator, the sector of insurance services, and leasing services did not provide STRs or provided them less frequently.

912. FIs are aware of the tipping-off prohibition when filing STRs and fulfil this obligation in practice. All FIs met by the assessors during the on-site mission demonstrated the existence of adequate systems and internal control procedures to ensure the confidentiality of the STRs sent, and no breaches of the tipping-off prohibition were identified.

Table 4.2. Number of STRs by obligatory criteria of suspiciousness and by criteria of dubiousness.

Category	2016		2017		2018		2019		2020		Total	
	By criteria	By suspicio usness	By criteria	By suspicio usness	By criteria	By suspicio usness	By criteria	By suspicio usness	By criteria	By suspicio usness	By criteria	By suspicio usness
Banks	32,669	191,242	63,920	171,571	109,560	134,864	281,869	99,360	563,894	133,737	1,052,002	730,774
Microcredit organisations	0	0	0	0	125	5	315	10	310	2	750	17
Pawnshops	0	0	0	0	81	1	97		107	0	285	1
Postal operator, electronic money system operators, and	0	0	0	0	0	0	0	0	0	41	0	41

payment system operators												
Postal operators	0	0	0	0	1	0	3	0	1	0	5	0
Professional participants	301	17	113	76	246	24	233	89	93	77	986	283
Insurers and insurance intermediaries	0	0	0	0	6	0	0	2	0	0	6	2
Commodities exchange members	600	598	187	237	393	9	620	73	261	8	2,061	925
Leasing companies	7	0	2	0	1	0	0	0	2	0	12	0

913. Between 2016 and 2020, the total number of filed STRs amounted to 1,055,923 by obligatory criteria of suspiciousness and 730,832 by obligatory criteria of dubiousness (which are also obligatory in the ICR of every FI and supplemented by FIs with their own inventions). Banks filed most reports which stem from a wide range of transactions, a large client base, and their active involvement in the risk assessment process. They accounted for 99.74% of all filed STRs. The other sectors accounted for 0.26% of STRs.

914. STRs are filed to the FIU according to a special form and via a secure channel that requires digital signing. Filing deadlines: a) dubious transactions (20 criteria) – after decision-making and analysis; b) suspicious transactions set out in the ICR (14 criteria) – until the end of the next day; c) by criteria associated with the List (3 criteria) – immediately.

915. Banks have coding for STRs related to dubious transactions that are enshrined in the ICRs. However, when STRs are filed to the FIU, general code 999 “Other indicators” is used, which the assessors believe to be making it difficult for the FIU to perform a proper analysis.

916. Banks automatised the process of identifying transactions that require internal control. Transactions that cannot be tracked by the software are tracked and analysed by employees of the bank’s compliance service based on comprehensive analysis (e.g., a client uses complex schemes, inconsistency with the stream of commerce, inconsistency with the type of activity or a client is being unusually concerned about confidentiality).

917. Monitoring scenarios for transactions subject to mandatory control are developed based on criteria established in the ICRs of the regulator. Some of these criteria correspond to the risks identified in the NRA and SRA. Further, relying on their own risk assessments, banks develop internal algorithms to monitor clients’ transactions. For instance, apart from the scenarios developed by the regulator, a bank introduces its own additional indicators of dubious transactions (13 additional scenarios). When a certain transaction of clients matches the existing criteria, designated employees take action to report this to the FIU.

918. A large number of breaches in banks that occurred in 2016-2017 (1 thousand and 1.6 thousand suspicious transactions that were not identified by obligatory criteria) stem from the absence at a few banks of comprehensive transaction monitoring procedures, analysis methods, allocation of responsibilities among employees, and other reasons. However, between 2018 and 2020, the effectiveness of banks' internal controls has improved and the number of unidentified suspicious transactions of the same category has significantly decreased.

919. There is another type of transaction which is different from suspicious transactions - these are dubious transactions. The average number of unidentified dubious transactions (this is a different category of criteria established in the ICR and additionally developed by FIs) remains high and stable from year to year – 2.2 thousand per annum. The Central Bank and the assessors note that banks do not fully understand the mechanism and procedures of identifying dubious transactions based on criteria established in the ICR. Another reason lies in the fact that a few banks do not have clearly defined monitoring procedures, analysis methods, and allocation of responsibilities among employees when it comes to identifying dubious transactions, which is also revealed during inspections conducted by the Central Bank.

920. The postal communication operator developed and implemented a suspicious transaction identification methodology. However local employees from this sector do not fully comply with their obligations to report their ML/TF suspicions. Representatives of the sector ascribe this to the fact that

employees of Uzbekiston Pochtasi JSC do not have a sufficient level of knowledge and awareness about ML/TF risks (notably, the understanding of vulnerabilities is good) and do not understand potential consequences (damage) that ML/TF-related illegal actions of clients and their counterparties can entail. In connection with an inadequate understanding of their obligations, insurance companies rarely submit STR. Supervision authorities should conduct outreach.

DNFBPs

921. As noted in previous sections, not all DNFBPs sectors file STRs and provide other material information. There are a few cases (4 STRs) of notaries submitting reports.
922. The DPMS sector which is characterized by an insignificant volume of performed transactions is primarily represented by small businesses and individual entrepreneurs. The average price of products sold rarely exceeds USD 1,000. Thus, the absence of STRs from the DPMS sector is explained by insignificant volumes of transactions performed by the vast majority of market participants.
923. The sector of lawyers does not file STRs to the FIU for there is no such need given that clients with ML/TF-related risks are denied services. However, there is also no information on denials of client service/transactions, which may be due to the fact that lawyers do not carry out transactions on behalf of their clients.
924. Notaries filed four (4) STRs, including one (1) STR in relation to a loan agreement (executory endorsement) which confirms that some notaries understand the risks. This fact is explained not so much by insufficient understanding of STR filing obligations as by the nature and volume of the services provided. Notaries understand ML risks associated with tools such as executory endorsement, however, most of the services provided (in the context of Recommendation 22) are related to the notarization of real estate purchase and sale transactions between individuals, and the average value of a property is insignificant, about USD 20,000.
925. Real estate agents are rarely involved in the actual execution of real estate transactions and often do not know the ultimate price of the transaction and the form of payment, which does not allow them to file an accurate STR. There is no need to file STRs when providing consulting services. This is also indicative of a perfunctory approach to performing AML/CFT obligations by real estate agents and, generally, that there is a weak practical understanding of the risk of real estate being used in ML/FT schemes. However, it should be noted that the services are mostly rendered to individuals and, as was noted before, the average cost of such transactions is not large.
926. The ICRs approved for all DNFBP sectors contain provisions that DNFBP employees should not disclose (or use to their personal advantage or in the interests of third parties) information that they obtained while performing internal control functions. All DNFBPs are fully aware of this obligation.

Internal controls and legal/regulatory requirements impending implementation

927. Reporting entities supervised by the CB successfully perform their internal assessments of the effectiveness of AML/CFT internal controls. Postal communication operators and exchanges organise their work in a similar manner. Some leasing companies create internal audit services and conduct ongoing monitoring of transactions, including AML/CFT. Joint-stock companies, limited liability companies, and additional liability companies with a relevant book value of assets are also required to create an internal audit service.
928. DNFBPs arrange for internal controls with due regard to the specific features of their activities. Requirements imposed on the organization and relating to internal control are established in the ICR approved by the supervisory authority in cooperation with the FIU. The ICR which were in force before 2021 establish a different scope of obligations for sectors because they are updated at different intervals. DNFBPs sectors demonstrate a diverse understanding of such obligations.

Financial institutions

929. All FIs have compliance departments or designated compliance officers as well as adequate internal control procedures. Designated officers are appointed by the executives (except for insurance

companies). Insurance companies, due to weaker understanding of ML/TF risks, do not appoint a separate compliance officer but assign internal AML/CFT control functions to existing employees (deputy chief of the company, head of the risk management department, security department or legal adviser).

930. Banks perform internal assessments of the effectiveness of AML/CFT internal controls by conducting annual internal audits. The audit results are reported to the higher management bodies represented by the Supervisory Council (Board of Directors). The management of banks performs ongoing monitoring and assessment of the effectiveness of internal controls at the bank accounting for varying internal and external circumstances and, if possible, improves internal controls in order to ensure effective operation. The higher management of banks, therefore, pays due attention to AML/CFT, which is effective, and the assessors made sure of that while visiting the banks during the onsite visit.

Case study 4.1. (Effective operation of a commercial bank)
The internal audit is subordinate to the Audit Committee of the Supervisory Council of a bank. Audit employees are appointed and removed from office only by the Supervisory Council. Any external attempt to influence the operation and independence of the internal audit is immediately reported by the Chief Auditor to the Audit Committee and the Chairman of the Supervisory Council. AML/CFT matters are considered and examined over the course of a year when segments of the bank undergo internal audits because audit programmes necessarily include relevant tests and matters.
At the end of each year, the Chief Auditor analyses risks and assesses necessary procedures (including AML/CFT matters) with a view to preparing an audit plan for next year. This process involves the assessment of the results of internal audits, including AML/CFT matters.
Apart from the audit, banks arranged for internal inspections of AML/CFT internal controls that identify breaches in the procedures and AML/CFT internal control rules, following which disciplinary action is taken with respect to employees who committed these breaches. Relevant statistics are available.

931. Monitoring conducted by exchanges and control of the compliance with ICR requirements by exchange members is regulated by state and internal legal acts. Authorized exchange personnel is appointed to control the work of exchanges member in the sphere of AML/CFT. The evaluators consider the said measures insufficiently effective since they do not form a comprehensive system of internal control/audit that should be developed.

932. The postal communication operator performs AML/CFT control in accordance with internal documents and other regulations. Internal control includes examination, monitoring, and inspections. The Postal Security Director heads the internal control unit. In 2017–2020, there was a quarterly monitoring report in all postal communication branches, divisions, and units. Certificates of deficiencies and recommendations on how to remedy breaches were issued following the examinations. The examinations were followed by outreach activities after which protocols were made and plans of action to remedy deficiencies and breaches were developed. This helped increase the effectiveness of the sector insofar as AML/CFT is concerned.

933. The securities sector referred to financial secrecy that does not make it possible to have a full picture of the financial standing of legal entities or individuals as one of the obstacles to effective control. Professional participants have no power to request information about clients of local or international banks. The assessors believe that the country needs to take action to eliminate this obstacle and create a comprehensive internal control/audit system in order to assess the effectiveness of FIs in this sector when it comes to AML/CFT.

934. The Law of the Republic of Uzbekistan "On Joint-Stock Companies and Protection of Shareholders' Rights" (Article 108) provides that joint-stock companies with a book value of assets exceeding one hundred thousand basic estimated values are required to create an internal audit service. Besides, limited and additional liability companies with a book value of assets exceeding UZS 1 billion are required to create an internal audit service (Article 45-1). FIs whose form of incorporation is JSC or LLC are governed by the above laws. The assessors find it difficult to reach any final conclusions in order to assess effectiveness for there is no information and necessary statistics on FIs where audit is performed to assess efficiency. At the same time, the assessors found that FIs, in which internal audit

services are being created, conduct ongoing monitoring of the transactions, in particular, as related to AML/CFT. As a rule, the executive body of the FI also conducts ongoing monitoring and assesses the effectiveness of the FI's internal control system, taking into account changing internal and external circumstances, and strengthening it as necessary to ensure effective operation. If deficiencies in the internal control system are revealed, the head of the FI's executive body ensures their timely elimination.

935. The internal control service of FIs operating in foreign financial groups is based on group policies, the requirements of which may be broader than those of domestic law. As for group approaches to internal control within domestic financial groups, there is no such statutory requirement (except for the requirement to bank groups in clause 61 of ICR dated May 23, 2017 No. 2886) and none is put into practice, which is inconsistent with the FATF Standards (R.18). The assessors could not assess the effectiveness of group approaches because there is no statistics on the number of financial (banking) groups and holdings operating in the Republic of Uzbekistan.

DNFBPs

936. All DNFBPs apply internal control procedures in accordance with the established ICR, which are mandatory for organizations' activities. The scope of the procedures applied varies depending on the sector and the requirements stipulated by the ICR. A designated officer appointed in all DNFBPs arranges the introduction and implementation of the internal controls and customer due diligence procedures in accordance with the ICR, develops and submits to the executives for approval an action plan for implementing internal controls, based on the special features of the organization's activities.

937. A designated officer of the DNFBP monitors the arrangement of the internal control system and the elimination of deficiencies identified in the organization's activities.

938. Audit organizations, in addition to the above, develop internal rules that stipulate the procedure for identifying, assessing, monitoring, managing, mitigating and documenting risks.

939. The relevant law directly states that submission in the prescribed manner of information on transactions with money or other property of legal entities and individuals or other information to a special authorized state agency does not constitute a violation of commercial, bank or other secret protected by the law, as mentioned by both notaries and lawyers.

940. The assessors come to the conclusion that the effectiveness of internal controls in DNFBPs depends not so much on the requirements for its arrangement, as on understanding the risks of a particular organization being directly involved in ML/TF schemes and understanding the ML/TF risks in general. This understanding is non-uniform, as noted above, and therefore, in general, the effectiveness of internal control procedures in most DNFBP sectors can be assessed as moderate.

Overall conclusions on IO.4

941. FIs demonstrated understanding of ML/TF risks and risk management measures based on NRA findings and training organised by the supervisory authorities. FIs understand their AML/CFT obligations, with banks, payment organizations, NBCI, exchange members and postal operator demonstrating a more complete understanding of such obligations among FIs. FIs apply CDD and EDD measures. A common problem is that STRs are not filed when it is impossible to complete CDD. EDD is not conducted in relation to domestic PEPs. FIs identify the BOs of clients at a sufficient level using the information provided by the client, with government databases and other publicly available sources used to verify data and for further study. FIs understand their TFS obligations.

942. Banks, exchange members, professional securities market participants, and NBCI, payment institutions actively perform an STR filing obligation in accordance with the established criteria of suspicion. The other FIs comply with this obligation to a lesser extent. FIs (except for banks and payment organisations) do not assess the risks of new technologies and/or products. All FIs have internal control. There is no audit and/or internal control over checks of the AML/CFT system (except

for banks and the postal operator), and there are no group approaches (except for the requirement to banks prescribed by ICR) to AML/CFT internal control.

943. Overall, DNFBPs largely understand their AML/CFT obligations given the specific features of the sector. However, the actual implementation of the established AML/CFT obligations is at a moderate level. Thus, all sectors arranged for internal control and comply with requirements of ICR related to basic CDD and work with the Lists, all DNFBPs demonstrated a good understanding of their obligations and the need to apply preventive measures in respect of CFT.

944. Obligations are often performed by DPMS and real estate agents in a perfunctory and superficial manner. Most DNFBP representatives did not demonstrate a sufficient understanding of BO-related matters or examples of EDD in practice. The main identified deficiency related to the implementation of the national AML/CFT requirements by DNFBP sectors is the failure to send STRs and other relevant information to the authorized body. This fact is explained not only by insufficient understanding of STR filing obligations but also by the nature and volume of the services provided.

945. Independent legal professionals and accountancy firms that provide company creation services operate in the country. These companies are not AML/CFT entities and therefore it is not possible to assess their impact on the effectiveness of the AML/CFT system. The Republic of Uzbekistan is advised to assess the risks of such services for AML/CFT purposes and, if necessary, to take measures to mitigate them.

946. It is important to mention that materiality of the DNFBP sectors in relation to FIs is insignificant in respect of the volume of services provided / transactions performed and in the context of ML schemes. Given the weight and importance of individual FI and DNFBP sectors, in the opinion of the assessors, the existing preventive measures allow for the conclusion that they are moderately effective.

947. **The Republic of Uzbekistan is rated as having a moderate level of effectiveness for IO.4.**

CHAPTER 6. SUPERVISION

Key Findings and Recommended Actions

Key Findings

Financial Institutions

1. Requirements for licensing or special procedure of registration with a supervisory authority for banks, NBCIs, professional securities market participants sufficiently prevent individuals with a record of conviction for the commission of certain categories of crimes (economic crimes and crimes against administrative order) from exercising managerial functions in financial institutions. The licensing requirements do not have provisions stipulating that the founders and beneficial owners of FIs should have a clean criminal record. However, in practice, the Central Bank effectively verifies that managers, founders and beneficial owners of the supervised FIs (banks, NBCIs, payment institutions) are not criminals. Supervisors effectively carry out preventive measures to identify unlicensed activities in the sectors of payment institutions, VASPs, and securities.
2. Supervisors, including the leasing associations and commodity exchanges (which carry out AML/CFT supervision along with the supervisors but are not government authorities), have been actively involved in identifying national risks and are well aware of the ML/TF risks in the supervised sectors, and they develop risk mitigation measures and communicate them to the private sector.
3. There is a strong level of supervision over the activities of financial institutions in the Republic of Uzbekistan. The Central Bank has implemented a risk-based approach to supervision for banks, payment institutions sector, and NBCIs. The Central Bank receives reports and carries out off-site and on-site AML/CFT inspections. AML/CFT supervision in the form of monitoring and inspecting activities are carried out by commodity exchanges in relation to exchange members and by the State Inspection for Control in the Sphere of Informatization and Telecommunications (Uzkomnazorat) in relation to the postal operator. In the remaining sectors, there are elements of AML/CFT monitoring, and control is partly carried out as part of general supervision.
4. Sanctions for violations of the AML/CFT requirements are actively applied to banks and NBCIs by the Central Bank, to exchange members – by commodity exchanges. The sanctions imposed are mostly proportionate and dissuasive, as evidenced by the statistics of violations detected. In the rest FI sectors, the measures applied are either occasional or are not applied at all.
5. The Central Bank, commodity exchanges and Uzkomnazorat effectively identify violations and entities eliminate violations in the supervised sectors. Cases of involvement of bank employees in money laundering schemes have been detected. In these cases, maximal fines are applied which are dissuasive and prevent repeated violations by FI employees.
6. The Central Bank takes a comprehensive approach to the training of its supervised entities on an ongoing basis. For the rest FIs, AML/CFT training, in particular, by sending information letters and guidelines, is regularly conducted by the FIU, supervisors, the leasing association and commodity exchanges, which evidences active work in this area.

DNFBPs

7. Due to the diversity of DNFBP sectors, the effectiveness of preventing criminals and their associates from owning and managing companies varies greatly from sector to sector. There is a high level of effectiveness in the lawyers and notaries sector and insufficient efficiency in other sectors, especially in the sectors of real estate agents and DPMS, where similar restrictions are almost completely missing.
8. It should be noted that almost all regulatory authorities have, in general, a sufficient understanding of the risks indicated in the NRA. The understanding of risks is kept up to date by the supervisors, in particular, due to the conduction of SRA. However, SRAs have not been conducted in all sectors.
9. When monitoring and controlling the supervised sector, the supervisors do not pay sufficient attention to the implementation of the AML/CFT requirements and mitigation of ML/TF risks. Due to the

almost complete absence of AML/CFT inspections, there is an obvious lack of control that cannot be compensated for by alternative means, for example, through the development of remote communication systems. The existing tools of off-site monitoring are not applied in practice to increase the law-obedience of the supervised entities.

10. Sanctions in the field of AML/CFT, particularly, the special article of the Code of Administrative Offences (179.3), have no dissuasive effect and no impact on the implementation of the mandatory AML/CFT requirements due to the lack of practical application.
11. The established practice of conducting training activities by the supervisors together with the FIU is highly efficient, which makes it possible to maintain a moderate understanding of AML/CFT risks and responsibilities to mitigate them.

Recommended Actions

Financial Institutions

1. To establish requirements in all sectors to prevent persons with a record of conviction for the commission of all categories of crimes (not only in the economic sphere and against the administrative order) and their associates from holding management functions and being beneficial owners of FIs;
2. To extend the special procedure for registration and/or licensing with the supervisory authority to leasing companies, and mobile communications providers conducting money transfers;
3. To extend legal AML/CFT requirements to activities of mobile communications providers conducting money transfers, the central depository, the stock exchange, and commodity exchanges and to determine requirements for insurance agents to ensure their compliance with the AML/CFT legislation;
4. To introduce risk-based AML/CFT supervision in the securities, insurance, and leasing sectors and to develop AML/CFT indicators in the exchange trading sector and postal money transfers sector that will be taken into account when assessing the level of FIs' risks for supervisory activities;
5. To maintain statistic records and analyze statistics of AML/CFT violations being detected (except for the CB) and apply in practice sanctions for violation of AML/CFT legislation by the reporting entities (except for the Central Bank, commodity exchanges);
6. To consider the possibility of arranging interdepartmental exchange between the Ministry of Finance and the Central Bank on the identification of suspicious transactions by banks relating to securities, by banks and microcredit organizations – relating to leasing activities.
7. Supervisors (other than CB) together with the FIU should strengthen feedback to FIs to improve the quality of STRs.

DNFBPs

8. It is necessary to implement control measures/monitoring, including sanctions when breaches are detected, in order to assess the actual implementation of the ICRs by the supervised entities (CDD, identification of suspicious transactions and customers, foreign PEPs, work with the lists and the TFS implementation, rejection of transactions/denial of services).
9. To increase the intensity of off-site monitoring and to include the reports directly related to the implementation of internal controls (high-risk customers, customers checked against lists, risk assessment of the services provided, the number of analyzed transactions, the number of transactions with indicators of suspicious transactions, etc.) in the list of reports provided by the supervised entities.
10. For more effective implementation of the RBA, consider the necessity of arranging the bilateral electronic exchange of information on an ongoing basis between the FIU and the supervisors relating to control and supervisory activities and identified violations. For the FIU, to submit information to the supervisors on the use of the personal account by the reporting entities, for the supervisors – to submit information on the results of monitoring and control.

11. To develop and implement a set of measures to enhance the capacity of supervisory staff in terms of understanding the AML/CFT responsibilities of the supervised entities.
12. To assess the sufficiency and proportionality of the number of employees of the State Assay Chamber involved in the AML/CFT control and supervisory activities to the size of the supervised sector and to consider the possibility of increasing the number of employees involved in the AML/CFT control and supervisory activities.

Immediate Outcome 3 (Supervision)

948. When assessing the results of supervisory activities under Immediate Outcome 3, the major weight was given to the banking sector as the most significant, which encompasses the vast majority of financial flows of both legal entities and individuals and also as a more exposed sector to ML/TF risks. For example, in 2020 total assets of banks amounted to USD 38,506.6 million (87% of the FIs assets), and the customer transactions volume amounted to USD 200,079.2 million (96.5% of the transactions of all FIs), see Chapter 1 for further details. Commodity exchange members have been identified as the second most important category of FIs which have an impact on the national AML/CFT system. The volume of transactions of FIs in this category amounted to 2.31% of the volume of all transactions of FIs of the Republic of Uzbekistan, and the ML/TF risks were rated as low, due to special features of the trading process on an exchange. The payment organization sector was identified as the third most important. The share of this sector in terms of transaction volume is less than 1% of that of all FIs (approximately USD 1.9 billion per year), but ML risks were rated as medium-high (TF risks were low). The contribution of the rest FI categories was deemed by the assessors as less significant.
949. Considering national ML/TF risks and the size of the sectors in terms of the number of participants and the volume of transactions, the precious metals and stones dealer (DPMS) sector is of significant importance among DNFBPs, notaries and lawyers are the second most important, and real estate agents are the third. The rest sectors (auditors and lotteries) have little weight in terms of the IO.3 assessment. For more details, see Chapter 1. As already mentioned, the DNFBP sector is characterized by an insignificant volume of financial transactions and services provided, and the total volume of transactions of the sector is not comparable with that of the FI sectors and comprises less than 0.1% of that of the FI sector, which makes it less significant than the FI sector for the purposes of the analysis.

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

Financial Institutions

950. Requirements for licensing or special procedure of registration with a supervisory authority for banks, NBCIs, and professional securities market participants sufficiently prevent individuals with a record of conviction for the commission of certain categories of crimes (economic crimes and crimes against administrative order) from holding a management function in financial institutions. Supervisors for all representatives of FIs, except for leasing companies and commodity exchange members, effectively check the qualification requirements for the executives of the institutions.
951. In addition to checking the qualification requirements, the CB (Banks, NBCIs) and the Capital Market Development Agency (securities market) check the business reputation of the founders and executives of FIs supervised by these agencies. Business reputation check includes checking whether they have an outstanding or unspent conviction. For this purpose, an inquiry is sent to the internal affairs authorities. In the rest FI sectors, the requirements for the business reputation of the founders and executives are missing and are not checked in practice, which is a significant deficiency for these sectors. There are also no preventive measures as a possible element in identifying apart from the CB.
952. In the banking sector, the CB has determined requirements for beneficial owner identification through a ban on registration of complex ownership structures and checking the BO of non-complex

ownership structures. Thus, the fulfilment of the requirement for identification of the beneficial owner of a bank, checking its business reputation is actually ensured and effectively implemented by the CB. The decision to issue preliminary permission to create a bank, a license to carry out banking activities and permission to purchase shares of a bank are taken by the Banking Supervision Committee on the basis of an experienced judgment. The decision is made after examining documents received from the applicants, in particular, additional information is requested, if necessary, (domestic, international) inquiries are sent, and meetings with applicants (shareholders, beneficiaries) are arranged.

953. There are examples when CB rejected a potential purchaser of the bank shares in excess of 20 percent because the purchaser failed to provide documented confirmation of the sources of funds and the CB identified a former conviction for an economic crime of the person being a business partner of the potential purchaser. This example demonstrates the work of the Central Bank in identifying also the associates of criminals.

954. For other FIs there are no beneficial owner identification mechanisms, there are no requirements for the business reputation of beneficial owners and their affiliated persons, and, accordingly, they are not checked in practice.

955. The CB has rejected candidates for heads of banks for the reasons indicated in table 3.1.

Table 3.1. Central Bank' refusals to endorse the appointment to senior positions in the banking sector in 2016-2020 (Persons)

Applications submitted	1,640
Of them rejected	102 (6.21%)
• Non-compliance with the qualification requirements	64
• Negligent attitude to the previously held position	23
• The candidate has been previously prosecuted by the court	15

956. In 2016-2020, the CB issued licenses to carry out banking activities to six banks. Two of them had one hundred percent of state-owned shares and four were private banks. Also, in 2016-2020 the CB reviewed 60 applications seeking permission to purchase the bank's shares, and positive decisions were made on 36 of them. The main reasons for refusals were related to the submission of an incomplete package of documents by the applicants.

Table 3.2. Statistics on examination of the beneficial owner of the applicant(s) seeking a permission to create a bank / purchase bank shares

	Number of issued approval documents					Examination of beneficiaries (number of applications in relation to which measures were taken to examine the applicants' beneficial owners)				
	2016	2017	2018	2019	2020	2016	2017	2018	2019	2020
Obtaining preliminary permission to create a bank;	1	1	1	1	2	1	-	-	1	2
Purchasing the bank's shares above the threshold[65] by the residents;	6	4	3	9	7	4	2	2	5	7
Purchasing shares of banks by non-residents	-	4	-	3	3	-	4	-	3	3

957. Other reasons for refusal relating to non-compliance with qualification requirements and business reputation requirements. Requirements for the business reputation of the founders of banks, microcredit institutions and pawnshops are established, but they do not include requirements for a clean record of convictions for the commission of all categories of crimes. Persons having an unspent conviction for the commission of economic crimes and crimes against administrative order only are not deemed to have an impeccable business and personal reputation. At the same time, subject to the

[65] Until 2020, the threshold is 20%; from 2020 - 5%

Law “On the Central Bank of the Republic of Uzbekistan”, the Central Bank has the right to use a reasoned judgment to assess the business reputation of direct and indirect founders (owners) of bank shares, including ultimate beneficial owners. This tool allows the Central Bank to recognize a person as having an improper business reputation, even if he/she has a record of conviction for the commission of other categories of crimes, thus expanding the scope of crimes. There are examples of refusals to approve the purchase of the bank’s shares and refusals to endorse the appointment to a senior position of persons with an improper business reputation on the basis of a reasoned judgment by the Central Bank. The right to use a reasoned judgment and reject persons with a record of conviction for any crimes (not only economic crimes) is deemed to be an effective mechanism.

Table 3.3. Statistics of examined applications for permissions to open a bank / purchase shares / reorganize a bank / open subsidiary banks, own branches and representative offices, participate in the creation of banks abroad

	Number of applications					Number of refusals				
	2016	2017	2018	2019	2020	2016	2017	2018	2019	2020
Obtaining preliminary permission to create a bank;	1	1	1	1	2	-	-	-	-	-
Purchasing the bank’s shares above the threshold[66];	26	4	5	11	9	20	-	2	2	2
Purchasing shares of banks by non-residents	-	4	-	3	3	-	-	-	-	-

958. In addition, in order to prevent illegal and fraudulent actions, the Central Bank has detected illegal use of the term “bank” or phrases with this term in the names of 17 organizations, and measures have been taken to eliminate and prevent such cases. Measures have been taken together with the registering authority (the Ministry of Justice) to adjust software settings to prohibit using the word “bank” in the name of a legal entity.

959. In 2015–2020, the Central Bank refused to issue a license to a total of 101 non-bank credit institutions (63 microcredit organizations and 32 pawnshops). The main reasons for the refusals were the submission of legally incompliant documents, failure to provide information on the origin of funds for the authorized capital and failure to provide information on the senior staff.

Table 3.4. Statistics of examined applications for permissions to open an NBCI

Procedures	Number of applications						Number of refusals					
	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020
Microcredit organizations	31	4	6	17	42	10	28	1	5	10	22	3
Pawnshops	8	10	8	18	11	4	4	5	8	9	5	1

960. The assessors evaluate the preventive measures taken by the Central Bank to work with the banking sector and the NBCI sector as significant.

961. The activities of exchange members require no license and are supervised by the commodity exchange. Exchange members undergo registration with commodity exchanges in the manner prescribed by the rules of exchange trading. Applicants for registration provide information about traders (employees of the legal entities), as well as constituent documents, which in turn are examined by the exchanges for compliance with the lists of persons involved or suspected of being involved in the financing of terrorist activities. There are no statistics or examples related to refusals and identified negligent participants, which constitutes a moderate deficiency.

962. The CB checks the qualification requirements for the executives of payment institutions. Until 2020 the sector has been unregulated since activities of payment institutions have been carried out by banks (except for 2 non-regulated payment system operators - Uzcard and Humo and 4 non-regulated payment institutions). In 2020, the Central Bank considered a total of 32 applications of payment institutions for a license, of which 12 applications were denied due to failure to submit a full package

[66] Until 2020, the threshold is 20%; from 2020 - 5%

of the required documents. In the same year, 2 applications of payment processors for a license were granted due to their full compliance with the legislative requirements. From June 1, 2021, state agencies, including the Central Bank, can independently request from the competent state authorities information on the criminal record, higher education and work experience of an individual through the interdepartmental integration platform Electronic Government. As of the on-site mission, 4 applications of payment institutions for a license were reviewed, and checks were carried out to prove the clean criminal record of the founders, beneficial owners and executives of the above applicants. The implemented measures are assessed as effective.

963. In the postal money transfers and money remittances sector, only JSC "Uzbekiston Pochtasi", the national postal operator, can provide money transfer services. To identify persons providing illegal (without a licence) postal money transfer services, in 2019, activities of 20 business entities providing postal services were audited, but the results showed no offenses. When executives of the national postal operator are hired, they are checked by sending inquiries to law enforcement authorities. The assessors highly assessed the country's work with the postal money transfers sector as related to protective measures.

964. There is evidence of LEAs detecting illegal hawala payments and prosecuting cash couriers involved in such payments. In addition to ongoing efforts, the competent and supervisory authorities need to make a concerted effort to identify the activities of payment systems categorised as hawala.

965. The DCMD identifies cases of unlicensed activities carried out as a professional securities market participant, on which materials are referred to law enforcement authorities (examples provided). The mass media, popular social networks, and feedback from the population are monitored to identify such violations.

966. For leasing services providers (other than banks and microcredit organizations), there are no licensing or special procedures of registration with a supervisory authority. The Ministry of Finance is the body that coordinates the activities of leasing companies. There is no special supervision, and the activities of leasing companies are monitored in accordance with the general procedure (by the tax authorities, etc.). Leasing transactions, including microleasing, can be carried out by banks and microcredit organizations which are effectively supervised by the Central Bank.

VASPs

967. Licensing of the virtual assets sector includes a number of restrictions aimed at minimizing the risk of VASP operations. Licenses to operate VAPSs are issued by the NAPM exclusively to foreign legal entities through the opening of subsidiaries or other enterprises on the territory of the Republic of Uzbekistan. Legal entities - residents of the Republic of Uzbekistan are not allowed to participate in the authorized capital of subsidiaries or other enterprises of foreign legal entities holding this license. Via VASPs, residents of the Republic of Uzbekistan may only enter into transactions for the sale of virtual assets. The Agency maintains an electronic register of licenses on its website.

968. In 2019–2021, 10 cases of activities carried out without a license were revealed in the VASP sector due to the active cooperation of the NAPM and the law enforcement authorities. Information for each of the cases was collected and transferred to the FIU, tax and law enforcement agencies for taking measures in accordance with the law. Criminal investigations were initiated in relation to 5 incidents. These preventive efforts to identify licensing-related violations are assessed as effective.

DNFBPs

969. Before 2021, all DNFBP sectors underwent the procedure for obtaining a license to carry out activities. However, Decree of the President of the Republic of Uzbekistan No. UP-6044 dated August 24, 2020 "On Measures to Radically Improve Licensing and Licensing Procedures" abolished licensing requirements for auditors, DPMS and real estate agents in the Republic of Uzbekistan from January 1, 2021. They undergo the registration procedure.

970. Notaries and lawyers operate on the basis of a license issued by the justice agencies. Compliance with the license requirements is also monitored by the justice agencies. Lawyers carry out activities only

within lawyer organizations, which are of the following types: law bureau, law office and bar association. A lawyer organization and a notary office are created by licensed lawyers and notaries, respectively.

971. Until 2019 there were only state notaries in the country who operated, in fact, as structural units of the Ministry of Justice that is why private notaries have not been registered. From 2019, for appointment to a position at the State Notary Office, the Higher Qualification Commission under the Ministry of Justice of the Republic of Uzbekistan has been holding a competition and qualification exam for the right to engage in the private notarial activity. In 2020, 225 applications were submitted, 54 applicants were selected, 161 did not score the required points, and 10 were refused. The refusals were not related to business reputation or other AML/CFT requirements.

972. Every year a fairly large number of lawyers pass the qualification exam successfully, and there have been no cases of refusal to grant the status of a lawyer.

Table 3.5. Applications for the Bar Qualification Exam

	2016	2017	2018	2019	2020
Applications submitted	384	324	841	644	415
Successfully passed	384	324	841	644	415
Refused	0	0	0	0	0

973. However, both notaries and lawyers cannot obtain a license and carry out activities in case of outstanding or unspent conviction (see analysis of TC). The absence of a refusal to pass the qualification exam also demonstrates that in practice there have been no instances of criminals (those with a criminal record) applying for a licence. Judicial agencies permanently carry out 150 audits of notary offices per year at the average and 250 audits of lawyer organizations, which is required by the Regulation on the Procedure for Auditing Activities of Justice Agencies and Institutions, according to which scheduled audits shall be carried out every 2.5 years. There were no revocations of licenses in the country, which demonstrates that no criminal cases have been initiated against notaries or lawyers. Thus, access of criminals to this activity is largely hindered.

974. The post of the head of a real estate organization can only be occupied by a person having a qualification certificate of a real estate agent. A certificate becomes invalid upon entry into force of a court decision stipulating the ban from holding a certain position or engaging in certain business activities. However, the procedure of issuance of a real estate agent's qualification certificate does not imply criminal record checks. There are no requirements stipulating criminal record checks of heads, founders and beneficial owners of real estate organizations. Also, nothing has been submitted to prove that the criminal background of persons with a real estate agent's qualification certificate is being checked.

975. One can conclude that if a real estate agent's qualification certificate is in place and the requirements for the composition of employees of a real estate organization are met, there are no obstacles to the creation of a company.

Table 3.7 Statistics related to issuance of permitting documents to real estate agents

	2016	2017	2018	2019	2020
Applications seeking a license	31	29	9	0	12
Approved applications seeking a license	31	29	9	0	12
Applications seeking a realtor's qualification certificate	775	793	516	169	369
Failed to pass the exam	498	572	358	151	256

976. From January 1, 2021, licensing has been cancelled, and the procedure for carrying out real estate activities will be determined after the adoption of a new regulation governing the admission of real estate agents to the market. Thus, at the time of the on-site mission, obtaining a special permit or special registration of real estate organizations was not regulated by any procedure. In 2011–2018, the authorized body has repeatedly sent materials to the governmental authorities, tax and law enforcement agencies regarding legal entities and individuals carrying out real estate activities without a license (a total of 38 letters).

977. The above factors cannot be dissuasive, that is, they cannot prevent criminals from running companies in the real estate agents sector. It should be noted that the absence of real estate agents' powers to engage in real estate transactions for and on behalf of their clients significantly reduces the possibility of involving this sector in the commission of ML or FT-related crimes. Another significant risk mitigation factor is the fact that registration of real estate transactions concluded between individuals is impossible without notarization.

978. The DPMS sector is rather heterogeneous, both in scale and in the types of activities of its participants, which entails significant differences in the levels of ML/TF risk in different market segments. During 2016–2020 the number of entities registered by the Assay Chamber exceeded 1,000 legal entities and individual entrepreneurs.

979. Jewellery production required a license and a registration certificate until 2021. From January 1, 2021, licensing was cancelled with the introduction of a notification procedure. It should be noted that only legal entities are empowered to trade in jewellery. In 2021, licensing remained only in relation to refining. Thus, market access in the sector has been simplified, which increases its vulnerability to misuse for ML purposes. In this sector, there are no criminal record checks (since the relevant legal requirements are missing) of executives, founders and BO of organizations, both during registration and subsequently, which also increases the sector's vulnerability. The sector is significant in terms of quantity, and the registration of new companies and individual entrepreneurs is quite active. At the same time, there have been no denials of licenses or registration certificates due to AML/CFT reasons. In general, access to the market is not hindered, and all the denials were related to non-compliance with the license requirements. There were no denials of manufacturing licenses, which also indicates that access to the market is easy.

Table 3.8 Statistics related to issuance of permitting documents in the DPMS sector

	2016	2017	2018	2019	2020
Applications seeking a (manufacturing) license	0	3	92	77	51
License denials	0	0	0	0	0
Applications for registration certificate (retail trade)	107	306	417	259	328
Registration certificate denials	0	165	288	75	61

980. Also, it should be noted that individual entrepreneurs are granted the right to label manufactured products themselves, which can be regarded as an ML/TF vulnerability of this sector, provided that control carried out by the Assay Chamber is insufficient.

981. Nevertheless, regarding precious metals turnover, the Assay Chamber actively cooperates with the SCC and the STC within the framework of the "Comprehensive Action Plan for Identifying and Disrupting Illegal Production and Sale of Jewelry" and has carried out about 800 joint inspections.

982. Business entities that have violated the branding and hallmarking procedure and sell jewellery not corresponding to the declared hallmark are entered into the register of unfair business entities of the jewellery industry and are subject to enforcement actions in the manner prescribed by the law, including termination of the license or other authorization document. At present, there are 4 organizations in this register; however, no licenses have been revoked.

983. Activities carried out without notification (previously – a license) are not systematically controlled by the Assay Chamber, and no examples of such practice have been provided. Nevertheless, in a number of cases such facts are revealed by law enforcement authorities, which indicates that there is a barrier in the country against conducting DPMS operations without proper registration.

984. In Uzbekistan, the law prohibits individual entrepreneurial activity in the provision of audit services. As of 2021, 96 audit organizations were registered in the country, which employed about 600 persons with a certificate of an auditor. The Ministry of Finance controls and supervises the activities of audit organizations. Auditors, as mentioned in the section on IO.4, practically do not provide services covered by the FATF Recommendations. Due to the existing requirements for the composition of members and heads of audit organizations (only an auditor can become the head and 51% of the authorized capital should belong to auditors), access of criminals to this sector is significantly hindered.

985. For all DNFBP sectors, there are no mechanisms for the identification of actual beneficial owners, and there are no requirements for the business reputation of beneficial owners and their affiliated persons.

986. Due to the heterogeneity of DNFBP sectors, the effectiveness of preventing criminals and their associates from owning and running companies varies greatly from sector to sector. One can say that in the lawyers and notaries sector, primarily due to special features of this activity and its legal regulation, access of criminals is sufficiently blocked, thanks to the requirements for a clean record of convictions and constant monitoring by the supervisor of the implementation of the laws on the legal profession and notaries. In this case not establishing BO at the time of registration, does not constitute a significant vulnerability, since activities are carried out either by notaries or lawyers themselves who are natural persons and act in their own interests or in the form of legal arrangements, in which only licensed representatives of the sector can become founders and executives who cannot be criminals due to existing restrictions.

Supervisors' understanding and identification of ML/TF risks

Financial Institutions

987. Supervisors, commodity exchanges and leasing associations (which are not supervisors, but actually operate as self-regulating organizations) have been actively involved in identifying national risks and are well aware of the ML/TF risks in the supervised sectors, and they develop risk mitigation measures and communicate them to the private sector.

988. In the 2019 NRA report, vulnerabilities of the banking sector were assessed on the basis of the activities of credit institutions in Uzbekistan as well as international factors, typologies, etc.

989. In addition to the NRA, ML/TF risks in the sector are identified through a sectoral risk assessment. In 2017–2018, the experts of the Central Bank together with the FIU conducted ML/TF risk assessment in the banking sector. The study was based on the methodology developed by an expert group from the Central Bank and banks. This document was approved by the Order of the Central Bank and communicated to the banks. The next sectoral risk assessment was carried out in 2019 by the Central Bank together with the FIU and banks. Based on the results of the sectoral risk assessment, a set of measures was developed to mitigate risks and improve the efficiency of the AML/CFT system in the banking sector, which was sent by a letter to all banks for implementation. During the on-site mission, the assessors were provided with information and confirmation on the implementation of the specified set of measures. Based on the results of the 2020 SRA, risks were updated, compared with predicate crimes and threats assessed by the law enforcement agencies, and measures to minimize risks related to the customers, products/services and their supply channels were developed and communicated to banks. Risk assessment is kept up to date due to regular updates on the ML/TF risks identified by banks; the updates are submitted to the Central Bank. In addition to information received from the supervised entities themselves, an updated sectoral risk assessment takes into account information received from the FIU based on the NRA results.

990. NRA in the payment institutions sector identified risks associated with unsupervised activities, namely, the use of money remittance systems, including for TF purposes (it should be explained that at the time of sentencing, the one payment system allowed transfers up to a certain amount with no reliable data about the remitter, which is not in line with the legislation of the Republic of Uzbekistan). As a result, measures were taken to disrupt activities of illegal payment systems, and supervision was established in 2020. Regulation of the payment institution sector has been implemented not long ago, so the SRA report was approved on June 7, 2021. The services most exposed to ML risk were the acceptance and execution of payments using a bank account, in particular, P2P transactions. Regarding TF risk, such factors as the recharge of foreign e-wallets and money transfers were mentioned. Measures were developed to minimize the identified risks. Taking into account the Central Bank’s experience and maturity of supervision, further work is ensured to communicate the developed measures to the sector and to implement them.

991. The assessors agree with the main conclusions of the SRA and the NRA and highly assess the proactive work of the Central Bank to identify and analyze the risks in the supervised sectors. In addition, it should be noted that the regulator started creating and implementing roadmaps to minimize the identified risks immediately after summing up the results of regular ML/TF risks assessments and before the approval of the national AML/CFT strategy which shows their promptness with regard to risk management.

992. In 2019, when preparing the NRA report, the Antimonopoly Committee provided answers to a questionnaire prepared jointly with commodity exchanges and exchange members. As part of this work, information was collected on the turnover of exchanges, the number of exchange members, the number of customers, the list of services of the exchange and exchange members, exchange members' procedure for establishing relations with the customers, risk assignment criteria, the possibility of anonymous transactions, the list of records kept by exchanges and exchange members, the number of violators and types of violations, on the conducted training activities. Besides the questionnaire surveys, face-to-face meetings were held to discuss the possibility of carrying out non-commodity transactions through exchange trading. Based on the results of the meetings, it was determined that, in line with the principles of securing exchange trading, payments are made only in case of deliveries. Vulnerabilities of exchange transactions are related mainly to focusing on the detection of suspicious transactions solely on the basis of threshold criteria and in some cases keeping transaction data for less than the specified period. In 2020, an action plan to mitigate risks was approved in the commodity exchanges sector, according to which deficiencies in the Internal Control Rules were eliminated; sanctions were revised that may be imposed by exchanges (Uzbek Commodity Exchange, RUACE) on their members.

993. In 2018–2021, other supervisors also conducted ML/TF risk assessments in the supervised sectors, following which risk assessment reports were prepared and submitted to the FIU. The report highlighted the key sector vulnerabilities that were taken into account in the national risk assessment. The assessors evaluate proactive work of the Information Technologies Development Ministry to identify and analyze the ML/TF risks in the postal money transfers sector and to eliminate the identified deficiencies as significant. To minimize the identified risks in the leasing services sector and to promote communication betweenthe parties with leasing organizations an Agreement on Special Partnership between the Ministry of Finance and the Leasing Association of Uzbekistan was signed on 2 March 2020. The assessors point out the great involvement of the Leasing Association of Uzbekistan in AML/CFT issues and actively work to minimize risks and improve compliance of leasing companies with the AML/CFT standards. Also, positively assessed its active communication with the supervisors based on the results of work carried out both at the stage of identifying and understanding the risks and in the development of measures to minimize them.

994. In most FI sectors (with the exception of the securities market and the insurance sector) the country has demonstrated an active position in identifying and understanding ML/TF risks, preparing programs to minimize them, as well as active interagency cooperation on this issue. The assessors consider the efforts of the Republic of Uzbekistan significant.

VASPs

995. The report on the results of the sectoral assessment of the money laundering and terrorist financing risks related to virtual assets turnover in the Republic of Uzbekistan was compiled by the NAPM and approved by the Decision of the IAC on April 12, 2021. Key findings based on the results of the sectoral risk assessment:

- Risks of ML with the use of VAs are low, while there are high risks of their use in predicate crimes, in particular, TF, illegal exchange of VAs, "shadow economy" turnover and the arrangement of "financial pyramids";
- The risk level is persistently affected by such factors as difficulties in establishing the identity when using VAs, the possibility of their decentralized turnover and conducting anonymous untraceable transactions.

996. The lack of technological solutions to eliminate these difficulties was mentioned, which causes vulnerabilities in the work of law enforcement and supervisory agencies and in the adoption of risk minimization measures.

997. The Republic of Uzbekistan has developed proposals to minimize ML/TF risks and introduce a risk-based approach in the field of virtual assets turnover, which includes adopting the law on the regulation of virtual assets turnover, imposing responsibility for violations related to virtual assets, strengthening human and expert resources of the relevant ministries and departments related to virtual assets, raising awareness of the population, developing licensing and registration procedures, strengthening international cooperation, etc. Based on the SRA results, Order of NAPM No. 10/1 dated April 16, 2021, on a risk-based approach was adopted, and the SRA report was submitted to the relevant ministries and departments for information and use in work. In addition, on May 20, 2021, the joint decree of the GPO, the SSS, the MIA and the SCC on cooperation in the field of VASPs control was developed and adopted.

998. The NAPM actively cooperates with the concerned ministries and departments and actively works to disrupt illegal activities related to virtual assets. 6 information letters were sent to law enforcement agencies on the facts of illegal activity related to virtual assets turnover identified by the Agency, 5 criminal cases were initiated, and 11 training events were held for law enforcement staff. The Agency's experts are involved in investigations and investigatory activities into illegal activities related to virtual assets turnover (10 facts at the time of the on-site mission). The assessors largely assess the efforts of the Republic of Uzbekistan to identify and minimize ML/TF risks related to virtual assets.

DNFBPs

999. Supervisors and most DNFBP sectors have been actively involved in identifying national risks, but only representatives of the DPMS sector found it difficult to indicate their role in the preparation of the NRAs.

1000. Understanding of risks by all supervisors is based primarily on the national risk assessment carried out in 2019, which is still relevant for Uzbekistan. All supervisors are aware of the NRA results and support its key findings.

1001. In addition to the NRA 2019, sectoral risk assessments were carried out in the sectors of notaries and lawyers, as well as auditors. Also, in 2020 sectoral risk assessment for the DPMS sector was prepared, which confirmed the NRA findings. SRA has not been carried out in the real estate sector, but the risks in this sector are understood by the regulatory authorities.

1002. Despite the conducted NRA and SRA, it seems that the results of these reports were not used to prepare new revisions of internal documents in the reporting entities, since no such examples were presented.

1003. The ICRs of all sectors stipulate the submission of an annual risk report to the FIU and to the supervisor, which allows supervisors to update information on ML/TF risks. This mechanism also allows supervisors to keep their understanding of risks up to date. However, to all appearance, in a number of cases these reports are of a formal nature, which is confirmed by poor understanding of ML/TF risks in practice by real estate agents and representatives of the DPMS sector, as well as by the lack of examples of identifying new risks and typologies based on the analysis of these reports. This fact is also related to insufficient monitoring by the supervisory authority and the lack of AML/CFT inspections.

1004. It should be noted that almost all regulatory authorities have, in general, a sufficient understanding of the risks indicated in the NRA. Assay Chamber representatives have a weaker understanding of the ML/TF risks, focusing mainly on the risk of buying stolen precious metal items, which nevertheless correlates with the NRA and SRA.

1005. In all sectors, the supervisors together with the FIU are developing methodological guidelines and recommendations for the supervised entities on risk management, new typologies and suspicious

activity indicators, which are communicated to the supervised entities to ensure comprehensive understanding of the ML/TF risks.

1006. The intensity of interaction between the supervisory authority and supervised entities directly affects not only the possibility of identifying new typologies by the supervisors themselves but also the understanding of risks in the DNFBP sectors. Thus, the deepest understanding of risks was demonstrated by lawyers, notaries and auditors due to the fact that supervision and interaction in these sectors are on an ongoing basis. The rest sectors demonstrate a more formal approach to identifying and understanding risks topical for the entity and the sector. In general, despite the satisfactory understanding of ML/TF risks by all supervisors, in most sectors understanding of ML/TF risks does not correlate with actual fulfilment of obligations in this sphere, such as classifying customers as high-risk, sending STRs, refusing to onboard customers which again is due to the lack of sanctions and supervision, in general.

Risk-based supervision of compliance with AML/CFT requirements

Financial Institutions

1007. In the CB the functions of methodology, coordination and control over the implementation of the internal control rules by all supervised entities, identification, assessment and minimization of the ML/TF risks are assigned to the Department for Coordination of Financial Monitoring and Currency Control in Credit Institutions, consisting of 3 departments. These resources are sufficient for risk-based supervision given the size of the banking sector and other supervised sectors.

1008. The CB demonstrated a full-scale model of risk-based AML/CFT supervision, which was implemented in 2020 and was based on detailed reports from the supervised sectors with a developed set of criteria, indicators, and control measures. This model covers banks, non-bank financial institutions, pawnshops, and the payment institutions sector.

1009. Until that time, the CB used a basic RBA, which was a part of prudential supervision, based on which both remote supervision and on-site AML/CFT inspections were carried out. Specifically, the elements of remote supervision of the basic RBA included:

- Analysis of dubious and suspicious transaction reports, high-risk customers, transactions related to offshore zones, customers who performed transactions using international bank cards in foreign countries, in particular, in offshore zones, in the amount equivalent to or exceeding USD 10 thousand, checking against the Lists and the implementation of the TFS, etc.;
- Analysis of the results of previous inspections, which took into account the type (CDD procedures, identification and submission of STRs, etc.), the number and the nature of violations, the state of the internal control system, including the effectiveness of its tools, etc.;
- Risks of banks (the risk of a bank being misused for ML/TF purposes), determined based on the results of the reports analysis and the results of the previous inspections.

1010. Based on the off-site supervision results, a report is prepared for submission to the management team, and after that, a decision is made to conduct a thematic inspection.

1011. During the on-site mission, the assessors were shown a matrix for determining the degree of supervision over the banks and practical examples of its application, as well as questionnaires and inspection reports. To calculate the weighted value, special coefficients have been developed, including individual AML/CFT indicators that correspond to the identified ML/TF risks, based on the level of significance of the indicators. Each reviewed indicator is rated on a maximum 10-point scale, and the points earned for the indicators are summarized by the weighted value. Based on the earned points, the level of potential ML/TF threat in banks is assessed (high, medium, low) and the level of the potential effectiveness of the banks' internal control system (high, medium, low).

Table 3.9. Number of Monitored Entities in Each Risk Category

	2016	2017	2018	2019	2020

	H	M	L	H	M	L	H	M	L	H	M	L	H	M	L
Commercial banks	20		7	19		9	15	9	4	12	14	4	4	21	6
Microcredit institutions	27		2	28		2	13		24	10		46	9		54
Pawnshops	46		1	46			8		47	15		46			64
Payment institutions														2	7

1012. It is worth noting that, according to the CB's methodology, until 2018 banks were divided into two categories only: high-risk and low-risk. Accordingly, low-risk banks were supervised remotely, while high-risk banks were subject to on-site inspections. In 2018, the CB's AML/CFT supervisory activities underwent some changes, namely the process of improving the supervisory methodology with regard to the risk-based approach began. According to the updated methodology, banks are divided into 3 risk categories based on the assessment results: high, medium and low level of AML/CFT/CPF supervision of banks is determined: 1) remote monitoring, which is divided into standard monitoring of low-risk banks (establishment and analysis of standard reports) and enhanced monitoring of medium-risk banks (establishment and analysis of additional reporting types) 2) on-site inspection (based on results of remote monitoring) of high-risk banks.

1013. The CB uses a wide range of monitoring tools to obtain information for a comprehensive assessment of the risk profile of banks: a system of indicators; remote communication system (reports submission); questionnaires; polls; testing; interviews with the management and the head of the bank's internal control department; analysis of Internet resources (including news channels, bank websites, social media, instant messengers, etc.) with regularly updated information related to the activities of banks, banking products and services.

Case study 3.2

During off-site monitoring, a case was revealed of illegal payment services being rendered by individuals through bank cards of Bank A with the involvement of employees of Bank A for subsequent conversion into cash of proceeds of crime.

Analysis of Bank A accounts showed that between January and May 2020, various individuals transferred a total of USD 63 million through 835 thousand transactions to bank cards of 39 people in order to place bets on foreign online betting sites.

Detailed examination of the above transactions revealed that for further withdrawals of funds received as winnings from the site, employees of Bank A were involved. Thus, in the period from March to May 2020, 39 people transferred USD 520 thousand, and these funds were used to purchase foreign currency and withdraw cash.

Bank A was penalized with a fine of USD 50,000 and according to the internal inspection results conducted by the bank, employment contracts were terminated with guilty employees of the bank in accordance with norms of legislation (in particular, a director of the internal control department, as well as bank employees who were attracted by clients to cash out their funds).

Information about the above case was transmitted to commercial banks in the form of index letters (as a typology) to prevent similar cases in the future and their application of appropriate measures in accordance with legislation.

1014. In the period of 2016–2020 the Central Bank conducted 190 inspections as part of risk-based supervision over banks:

- 33 comprehensive inspections as part of the general inspection, including on AML/CFT issues;
- 40 comprehensive inspections exclusively on AML/CFT issues (mainly in 2016–2017);
- 117 thematic inspections exclusively on AML/CFT issues (mainly in 2019–2020).

1015. The RBA methodology in the payment institutions sector and NBCI is similar to that of the banking sector, except for the use of sector-specific indicators. Monitoring of the payment institutions sector has been implemented not so long ago, that is why it is impossible to determine the effectiveness of monitoring since by the time of the on-site mission no inspections had been carried out and no sanctions had been applied. It should be noted that during the period under review, the Central Bank

annually checked all NBCI that fell into the high-risk category as part of on-site inspections, remote supervision was also carried out within the framework of the RBA model.

1016. The assessors believe that the presented system allows the Central Bank to carry out risk-based AML/CFT supervision of the supervised sectors (banks, payment institutions sector and NBCI).

1017. Observance of the ICR requirements by two commodity exchanges is monitored and controlled by the Antimonopoly Committee (1 employee), observance of the ICR requirements by the exchange members – by exchanges (27 persons are involved). These resources have been assessed as adequate. Exchanges, within their powers, establish and take measures against exchange members who have violated the ICR requirements. These measures are enshrined in the rules of exchange trading. Off-site and on-site inspections are not carried out in the sector due to a lack of a legal basis for conducting AML/CFT inspections, which the assessors deemed to be a deficiency.

1018. At the same time, since 2019, the brokers of the territorial branches of the exchanges have been charged with the task of controlling and monitoring the implementation of AML/CFT/CPF programs by responsible employees of the exchange members. Exchange employees examine activities of the exchange members, prepare the results of the examination, and, if necessary, impose sanctions on the exchange members. Based on the letters from the FIU, violations committed by the exchange members are also revealed, for example: in 2016 – 2, in 2018 – 5. Sanctions were applied to each exchange member-violator, in particular, they were suspended from exchange trading for a period of 3 to 6 months.

1019. In order to strengthen the monitoring of exchange members' compliance with the ICR, the Antimonopoly Committee distributed statistical tables to the exchanges. The tables are to be filled out monthly and submitted to the Antimonopoly Committee (Ref. No. 602-04-22 dated April 14, 2020), which, among other things, requires information on violations and sanctions applied. The collection of statistical data allowed the exchanges to enhance control over the implementation of the ICR by the exchange members, and the analysis of the statistical data provided by the Antimonopoly Committee enabled to assess the effectiveness of the exchanges. These measures can be deemed to be the start of the implementation of the AML/CFT RBA.

1020. Since January 2021, standard forms of documents on recording the CDD measures have been distributed. The forms were developed by the Antimonopoly Committee jointly with the exchanges. At the end of each month, JSC Uzbek Commodity Exchange conducted documentary examinations of selected exchange members to find out how they record CDD procedures and assess the risks of transactions. At the initial stage, the criterion to start the examination was the largest transaction amount in each region. During the 5 months of 2021, JSC Uzbek Commodity Exchange carried out 130 documentary examinations.

1021. In the securities and insurance sectors, there are elements of AML/CFT monitoring by supervisory bodies (4 staff from the Insurance Market Development Agency and the Department of Capital Market Development of the Ministry of Finance are involved), and control is partially carried out within the framework of general supervision without specialization on indicators in the AML/CFT field.

1022. In order to monitor the compliance of leasing organizations with AML/CFT legislation, the Agreement on social Partnership between the Ministry of Finance (1 person is involved in the supervision) and the Leasing Association of Uzbekistan is being implemented, thus monitoring will be carried out by both the Ministry of Finance and the Association. The results of such a state-private partnership on the coverage of control measures of the postal operator are assessed as successful. At the same time, in the sectors of securities, insurance and leasing organizations, RBA is not used, which is a significant shortcoming.

VASPs

1023. Regulation by the NAPM in the field of VA turnover is conservative and complies with the latest innovations in the FATF international standards. The only registered VASP has not actually started its work. Active work is underway to curb illegal activities. NAPM, with the technical assistance of

the local office of UNODC, has been working to improve the effectiveness of supervisory activities using modern information technologies, in particular, an agreement has been reached on the pilot use of the software by employees of the VASP that provides monitoring, analysis and visualization of transactions with VA. Considering the factors presented and the absence of entities of supervision, at the time of the on-site mission, the efforts of the VASP regulator are evaluated by assessors as significant.

DNFBPs

1024. In the Republic of Uzbekistan, since April 1, 2018, a moratorium on inspections of financial and economic activities of business entities has been in effect for 2 years, with exception of inspections conducted in criminal cases and in connection with the liquidation of legal entity. After the end of the moratorium (in 2019), inspections were also difficult and not carried out due to the lack of indication of control in the AML/CFT/CPF field in the approved List of inspections carried out by notifying the authorized body by registering them in the Unified Electronic Registration System of Inspections (UP-5490-son dated 07/27/2019 "On measures to further improve the system for the protection of the rights and legitimate interests of business entities"). The President's Decree No. UP-6252 dated 06/28/2021 included the implementation of AML/CFT/CPF control in the list of inspections, implementation of which is possible only with the use of the risk-based approach.

1025. Due to this fact, as well as due to the beginning of the SARS COV-2 pandemic in 2020, there are no inspections of DNFBPs since 2018, with the exception of the lawyers and notaries sectors, where inspections are mandatorily carried out every 2.5 years in accordance with the current sectoral legislation. A risk-based approach is not implemented in this context.

1026. The Assay Chamber and the State Assets Management Agency, however, mention on-site preventive work with the sector entities, which is not regulated and carried out without documentation and is primarily related to consultations on the implementation of the sectoral legislation.

1027. Regarding precious metals turnover, the Assay Chamber actively cooperates with the SCC and the STC within the framework of the “Comprehensive Action Plan for Identifying and Disrupting Illegal Production and Sale of Jewelry” and has carried out about 800 joint inspections. These measures reduce the risk of conducting supervised activities illegally, however, they are not related to monitoring compliance with the AML/CFT legislation requirements by the reporting entities.

1028. The submitted inspection programs of supervisors cover organizations’ compliance with the internal control rules, however, due to the ban on inspections, there are no examples of actual control over compliance with the AML/CFT requirements. Nevertheless, in a number of cases, compliance with the sectoral legislation has been inspected, and concurrently the availability of internal AML/CFT documents has been examined. However, AML/CFT issues are not monitored separately, and no sanctions are applied.

Table 3.10

	2016		2017		2018		2019		2020	
Type of inspection	On-site	Off-site	On-site	Off-site	On-site	Off-site	On-site	Off-site	On-site	Off-site
Persons engaged in transactions with precious metals and precious stones	17	0	19	0	138	509	44	411	10	379
Notarial offices (notaries)	166	0	147	0	146	0	143	0	0	850
Lawyer organizations (lawyers)	343	0	314	0	354	0	295	0	0	0
Audit organizations	12	0	29	0	1	0	0	0	0	0
Institutions conducting lotteries and other games of chance	0	0	1	0	0	0	0	3	0	0
Persons providing services and engaged in transactions related to purchase and sale of real estate	2	0	0	0	0	0	0	0	0	0

1029. In the DPMS sector, inspections were carried out in accordance with the requirements of Decree of the Cabinet of Ministers dated 09/30/2017 No. 777 "On the Procedure for licensing activities for the production of jewellery and other products made of precious metals and precious stones" and in accordance with requirements of Decree of the Cabinet of Ministers dated 05/29/2018 No. 399 "On Approval of the Regulations on the Procedure for issuing a registration certificate for work with precious metals and precious stones", where AML/CFT issues were not touched upon.

1030. In the lawyers and notaries sector, the arrangement of internal control is inspected, namely the existence of the ICR and other internal documents, without paying due attention to measures actually applied by entities, such as conducting CDD, identifying suspicious transactions, etc.

1031. A risk-based approach is not applied to the control and supervisory activities. At the same time, there are elements of the risk-based approach to supervision in the work of a number of control bodies, based on the development of electronic accounting systems for the supervised entities:

- The State Assets Management Agency conducts risk assessment of the supervised entities based on the submitted reports on the volume of transactions and information on the implementation of the AML/CFT requirements, using the electronic platform "Appraisal and Real Estate Activities". Registration of entities is carried out on the basis of the system as well as communication with them.
- The Ministry of Justice and the Ministry of Finance have similar mechanisms in the notaries sector (AIS Notary) and in the auditors sector (PK "Audit"), respectively.
- Lawyers submit reports via secure e-mail "E-XAT". It should be noted that, in this case, reporting is not related to AML/CFT issues, but nevertheless, it allows assessing the risks of entities associated with the services they provide.
- Representatives of the Assay Chamber mention differences in ML/TF risks among the reporting entities (purchase and sale – higher risk, manufacturing – lower risk), however, in practice, the risk-based approach is not implemented and used.

1032. However, these elements of the risk-based approach are not applied in practice due to the actual absence of inspections in the majority of DNFBP sectors. It should be noted that with the adoption of the Decree of the CM No.402 in June 2021, supervisory authorities are able to carry out risk-based monitoring and control, which in the future, will increase the effectiveness of control in the DNFBP sectors.

1033. One should also mention that there is a clear disproportion between the control-related resources of the Assay Chamber in the field of AML/CFT compliance (3 supervisors, no remote monitoring tools) with the risk scope and risk level in the sector. The remaining sectors have a sufficient number of supervisors (taking into account staff in regional supervisory units) who can be charged with AML/CFT compliance monitoring and remote monitoring tools are available.

Remedial actions and effective, proportionate and dissuasive sanctions

Financial Sector

1034. Supervisory authorities have administrative and other sanctions in the form of fines, withdrawal of license/exclusion from the register. Enforcement actions and sanctions for violations of the AML/CFT requirements are actively applied by the Central Bank in respect of banks and NBCI. The sanctions being applied are generally proportionate and dissuasive, as evidenced by the statistics on the decrease of the revealed violations. However, since the new supervision model has been applied for a short time (less than a year), the statistics on inspection activities and applied sanctions over the past year have not undergone significant changes.

1035. Identified violations in the banking sector mainly relate to such mandatory elements of AML/CFT internal controls as customer surveying procedures (CDD procedures and data keeping), identification of suspicious transactions, and STR completion procedures). Based on the results of inspections in 2020, 27 of 28 banks received instructions to rectify violations. It should be noted that

in 2019 17 of 25 inspected banks received instructions, in 2018 - 4 of 18 inspected banks received instructions, in 2017 – 8 of 19, and in 2016 – 15 of 25.

1036. The total amount of fines imposed on banks in 2015 and 2016 amounted to 640 million UZS (approximately 60 thousand US dollars, 14 banks) and 230 million UZS (approximately 21 thousand US dollars, 10 banks). In 2017, fines increased to 1.52 billion UZS (145 thousand US dollars, 11 banks) due to an increase in the minimum authorized capital of commercial banks. Another factor that caused the increase in the amount of the collected fines was the increased number of violations in identifying suspicious transactions and sending reports about them to the financial intelligence unit. In particular, the maximum penalty was collected from one bank (1 billion UZS, about 95 thousand US dollars) for non-compliance with AML/CFT internal control procedures (CDD, data keeping, STRs). No repeated violations of a similar nature were identified, which shows the dissuasive nature of penalties.

1037. In 2018, according to the results of inspections carried out in all areas, the total amount of fines was 20.5 billion UZS, of which 4.3 billion UZS (408 thousand US dollars) were related to violations of the AML/CFT legislative requirements. It should be noted that in 2018, a maximum fine of 1 billion UZS or 95 thousand US dollars was collected from three banks. In 2019, the total amount of fines for violations of the AML/CFT legislation amounted to 2.3 billion UZS (218 thousand US dollars), in 2020, 3.5 bln UZS (323 thousand US dollars).

Case study 3.4

In the course of supervisory activities, a sham transactions scheme was identified that involved depositing proceeds from export contracts through the bank's cash desks, where the receipts and expenditure of foreign cash were without the physical presence of currency. It should be noted that the above scheme can be used for ML purposes by creating artificial proceeds under sham or overpriced contracts and by mixing criminal proceeds with legitimate activities. In this regard, according to the results of inspections, 3 banks were penalized with the maximum fine (1 billion UZS, about 95,000 US dollars) for a total of 3 billion UZS, about 282,000 US dollars.

1038. Also, in the period from 2016–2020, based on the results of inspections carried out by the Central Bank, the banks applied disciplinary measures against the staff responsible for internal controls:

- In relation to managers: penalties in 26 cases, reprimands in 7 cases, and dismissal from office in 5 cases;
- In relation to employees: employees were dismissed from their offices in 141 cases, employees reprimanded in 137 cases, and fines imposed in 58 cases.

Table 3.13. Disciplinary actions taken against the managers and employees of the bank

Year	Number of employees dismissed from their offices	Number of reprimanded employees	Number of employees from whom fines were collected
2016		45	1 419
2017		63	1 035
2018		51	2 665
2019	1	14	598
2020	14	16	229
Total	15	189	5 946

1039. In 2018, a sharp increase in the number of employees subject to penalties due to a large number of thematic inspections conducted by the CB during this period resulted in fines of 4.3 trillion UZS (about 352 million USD) for banks, which is 65% and 45% more than in 2017 and 2019, respectively. It should also be noted that in 2018 inspections were conducted in large state banks, which in practice are more likely than other banks to impose penalties on their employees. The average fine includes a one-time fine of no more than thirty percent of average monthly earnings and forfeiture of the right to receive bonuses for five to six months. The average pay in the banking sector is 500 USD to 700 USD.

1040. The CB has a wide range of sanctions-imposing mechanisms and applies them in practice in the banking and NBCI sectors. The size is proportionate and has a dissuasive effect on the supervised sectors (except for payment institutions as the sector became regulated from 2020), the supervised entities develop action plans to eliminate the violations identified and shortcomings of work and submit reports of their implementation to the CB.

1041. In the stock trading sector, the deficiency is that exchanges are not subject to sanctions of the Antimonopoly Committee. But, commodity exchanges apply penalties to exchange members for violations of exchange trading rules, including in the field of AML/CFT. In 2016 and 2018 Uzbek Republican Exchange suspended 2 exchange members from trading for 6 months, in 2018 Republican Universal Agricultural Commodity Exchange suspended 3 exchange members for 3 months and in 2021 suspended 2 exchange members until deficiencies are corrected. This measure is quite effective for representatives of commodity exchanges as it directly affects the sphere of their business interest.

Case study 3.5

During the examination of the transaction documents, it turned out that exchange members, when conducting CDD, did not request a document certifying the state registration and a copy of the charter from the customers. Exchange members were temporarily suspended from trading until the deficiencies were eliminated. Further, 4-11 days later, after exchange members presented customer documents for review, they were allowed to trade.

1042. The postal operator is monitored by Uzkomnazorat (the State Inspection for Control in the Sphere of Informatization and Telecommunications) by a continuous method. The inspection body issues instructions to eliminate the identified violations at postal facilities and gives written explanations and recommendations to eliminate shortcomings in the work of the staff. Based on the results of joint inspections conducted in 2018–2019, disciplinary sanctions (reprimand, fine, dismissal) were applied against 53 persons who violated the internal control requirements. The conducted joint inspections have a positive impact on the professional development of the staff and the provision of postal services, and as a result, the postal operator, on its own initiative, asks to renew the agreement with Uzkomnazorat annually and to continue inspections of the subdivisions' compliance with the ICR requirements.

1043. In the securities sector, fact of criminal activity of an investment intermediary was revealed during the specified period.

Case study 3.6

In 2019, the Agency revealed the following fact of crime in the actions of an investment intermediary.

In November-December 2018, the deputy director of investment intermediary LLC "D", in order to steal alien property, sold the shares controlled by LLC "D" and owned by citizen N and transferred the received money to his own bank card, thereby inflicting damage on citizen N in the amount of 663.4 million UZS (approximately 62 thousand US dollars).

At the same time Sh, the internal controller of LLC "D", in violation of the requirements of the securities market legislation, failed to inform the head of the professional participant and the authorized state body for securities market regulation about the revealed violations.

The collected materials were sent to the DCEC, and as a result, a criminal case was initiated, and by the verdict of the Mirabad District Criminal Court dated September 9, 2019, A, Deputy Director of LLC "D", was found guilty of committing a crime under Art. 167, Part 3, par. a) of the CC (grand theft by misappropriation or embezzlement of alien property entrusted to or under the supervision of the guilty person), and a penalty was imposed on him.

Subject to the verdict, given that in accordance with Article 23 of the Law of the Republic of Uzbekistan "On Licensing of Certain Types of Activities" the license is terminated, in particular, in cases of systematic or one-time gross violation by the licensee of the license requirements and the terms and conditions of the license agreement, X, Director of LLC "D", whose job responsibilities included management of the company's activities, control, organization of work and effective cooperation of all the employees, Deputy Director A, as well as internal controller Sh were deprived of qualification certificates by the Agency's Decision No. 05-26 / 02 dated January 27, 2020. The Agency also brought a

claim to the court to deprive LLC "D" of the license to carry out activities of a professional securities market participant.

1044. In 2017-2018 17 penalties were applied against insurers for violation of the requirements of the internal control rules related to violation of the deadlines for submitting information on responsible AML/CFT officials to the Ministry of Finance, which had a dissuasive effect and in 2019-2020 no such violations have occurred again:

- In 2017, 7 companies were penalized for a total amount of USD 8,972;
- In 2018, 6 companies were penalized for a total amount of USD 4,146.

VASPs

1045. The only licensed VASP in the country has not started its operations yet, therefore, at present, there is no information on the applied corrective measures or sanctions.

DNFBPs

1046. Sanctions for violations of the AML/CFT requirements are not applied against DNFBPs in practice, therefore, it is impossible to assess their dissuasive effect. This can be explained both by the fact that inspections have not been conducted in most sectors since 2018 and by the fact that during inspections until 2018, the issues of compliance with the AML/CFT requirements were not fully assessed.

1047. In the lawyers and notaries sectors, where inspections are carried out every 2.5 years and AML/CFT issues are included in the inspection program, no violations have been identified. As previously mentioned, this is due to the fact that only internal documents developed for AML/CFT purposes were inspected. Also, there were no cases of license revocation or other measures to terminate the operation of an organization because of the revealed violations.

1048. However, in sectors such as lawyers, notaries, and auditors, alternative dissuasive sanctions (not involving the imposition of a fine under the CoAO) are in place because of reputation and licensing requirements. But not all of the rest supervised entities could report the availability of special administrative sanctions for failure to comply with the AML/CFT requirements.

1049. Also, criminal sanctions for money laundering and terrorist financing have a certain dissuasive effect due to the fact that DNFBPs associate failure to take measures aimed at identifying persons involved in TF/PF with possible consequences in the form of criminal prosecution for terrorist financing. This opinion has been expressed by the DPMS sector, lawyers, notaries, and real estate agents. Thus, it can be concluded that criminal sanctions indeed have some effectiveness, especially in such high-risk sectors as the DPMS sector.

1050. However, it should be noted that sanctions in the field of AML/CFT, particularly, special article of the Code of Administrative Offences (179.3), have no dissuasive effect and no impact on the implementation of the mandatory AML/CFT requirements due to the lack of their practical application.

Impact of supervisory actions on compliance

Financial Institutions

Table 3.14. Information on the results of inspections of the AML/CFT internal controls in banks conducted by the Central Bank

Violation / year	2016	2017	2018	2019	2020	Total
Unidentified suspicious transactions	1,570	1,008	301	56	75	3,010
Unidentified dubious transactions	2,240	2,111	2,069	2,542	2,258	11,220
Questionnaires not kept for a specified period (5 years) (number of questionnaires)	29,792	1,776	52	1,548	1,643	34,811
Number of customers for whom the questionnaires were not created	210,523	102,096	203	1,613	1,611	316,046
Number of questionnaires that were completed incorrectly or incompletely	19,124	35,649	13,259	21,408	27,523	116,963

Violation of CDD procedures during incidental transactions	17,252	7,206	1,133	4,365	7,582	37,538
Number of customers with no risk level assigned	150	1,700	107	740	1,184	3,881
Number of customers not classified by banks as high-risk in accordance with the ICR requirements	1,604	3,069	1,450	2,198	1,975	10,296
Number of employees responsible for internal control who did not upgrade their skills	175	227	10	45	85	542
Number of branches that did not organize workshops for the bank employees	72	66	2	31	85	256
Violation of data update requirements (number of cases)	2,042	2,050	301	680	507	5,580
Total	284,544	156,958	18,887	35,226	44,528	

1051. The CB identifies violations and entities eliminate violations in the supervised sectors. The identified violations mainly relate to such mandatory elements of AML/CFT internal control as questionnaire survey procedure (CDD and data storage procedures), identification of suspicious transactions, and procedure for STR completion. Cases of involvement of bank employees in money laundering schemes have been detected. In these cases, maximum penalties apply (see the core issue 3.4). Changes in Table 3.14 (reduction of the number of violations) are related to the supervisory authorities' actions and the dissuasive nature of the sanctions. In 2018, the total number of breaches of the CB's AML/CFT internal control system at banks amounted to 18.9 thousand, which is 8.3 times less than in the previous year. These dynamics were influenced by a sharp decrease in the number of violations related to failure to keep the questionnaires within the prescribed period (5 years), failure to form the questionnaire, as well as incorrect or incomplete completion of the questionnaires. However, in 2019 and 2020, the figures for the above-mentioned types of breaches increased. This is due to a technical failure of the ABS, namely, some banks were still working on switching from one ABS to another. In most cases, this problem was resolved during the audit by making an inventory and restoring the relevant questionnaires from back-up databases or from the old ABS.

Case study 3.7

During the inspection of the bank and its branches the following deficiencies were identified: in 35 cases no proper checks of the customers were performed for occasional transactions, and there were revealed violations of the ICR requirements for completing and keeping customer profiles; 33 bank customers were not classified as high-risk customers; 195 suspicious transactions conducted by several related entities were identified and reports were not filed to the FIU; 14 entities conducted 413 suspicious transactions related to illegal cash withdrawals, which were also subject to checking and filing to the FIU. The aforementioned violations were primarily related to deficiencies in the organization of the AML/CFT internal control system, in particular the lack of comprehensive procedures for identifying suspicious and dubious transactions, i.e. monitoring procedures, methods of analysis, distribution of responsibilities, etc. As a result, the maximum amount of penalties established by the legislation was applied to the bank, namely 1% of the established minimum amount of the charter capital of the bank – 1 billion UZS (93 thousand US dollars).

1052. The dynamics of violations show a decrease in the total number of deficiencies in the internal control system in the banking sector. . The assessors believe that the CB's supervisory activities and sanctions mechanisms have a positive effect on the banking sector and banks better understand the profile risks and take their responsibilities seriously, however, moderate improvements are needed - additional outreach work is required related to questionnaire survey of the customers, identifying suspicious transactions and CDD procedures for occasional transactions.

1053. Exchange members are subject to penalties from commodity exchanges, while the exchanges themselves are not, since they are not AML/CFT entities. In order to resume the activities of an exchange member, traders are tested again and persons responsible for compliance with the ICR are interviewed and instructed. If the results are positive, the exchange member is granted access to trading. All of the aforementioned violators have resumed their activities upon the expiry of the

suspension period. Statistics on coverage of the exchange members by control measures and rarely applied measures in the form of suspension from trading prove their efficiency and dissuasive nature.

1054. Due to the recent extension of monitoring to the sector of payment organizations, it is not possible to determine the effect of the supervisor's actions on the level of compliance with AML/CFT requirements, since no inspections were conducted and no sanctions were imposed at the time of the on-site mission.

1055. The analysis of the dynamics of identified violations indicates an improvement in the compliance of NBCIs with internal control rules and an increase in the effectiveness of the AML/CFT regime. A large number of questionnaire-related violations in 2019 is explained by a software failure due to the fact that microcredit organizations and pawnshops were switching from one automated system to another.

Table 3.15. Types of violations of AML/CFT legislative requirements by NBCIs

	2016		2017		2018		2019		2020
	CDD	Other types	CDD	Other types	CDD	Other types	CDD	Other types	Other types
Microcredit institutions	12	500	1	44	24	40	67	628	236
Pawnshops	0	31	0	98	0	10	3	5219	

1056. The results of inspections, examinations, and monitoring by the State Inspection on Control in the Sphere of Informatization and Telecommunications show improved compliance with the internal control requirements (in 2018 there were 83 violations, in 2019 – 65, in 2020 - 30). Upon the results of the examination, outreach has been conducted by regional branches of the Uzbek postal operator; action plans to eliminate deficiencies and violations have been developed.

1057. Measures applied by supervisory authorities in respect of the rest FIs (leasing, insurance companies, and professional securities market participants) have been non-recurring and occasional.

DNFBPs

1058. The CAO stipulates liability in the form of a fine for the guilty officials of organizations for failure to comply with AML/CFT measures. The size of the fine can reach more than 1,000 US dollars, which should have an impact on the proper implementation of the AML/CFT requirements by the supervised entities. These sanctions are proportionate and dissuasive based on the size of the average nominal pay (as of Q3 2019 according to the State Statistics Committee) in the Republic of Uzbekistan, which is 2,217,827 UZS or 231 USD, taking into account the USD to UZS exchange rate as of April 7, 2020.

1059. However, due to the fact that the said sanctions have not been applied in practice, and due to the non-detection of violations of the AML/CFT requirements in DNFBP sectors, it is possible to assess the dissuasive role of the sanctions in DNFBP sectors as low.

1060. At the same time, it should be noted that, undoubtedly, work jointly conducted by the supervisors and the DCEC in order to raise awareness of the entities carried out in the form of workshops, conferences, and various methodological recommendations have an impact on compliance with the mandatory AML/CFT requirements (for more details, see IO3).

Promoting a clear understanding of AML/CFT obligations and ML/TF risks

1061. The assessors emphasize the country's active engagement with the private sector both in the FI sectors and DNFBP sectors. Training and informational activities on urgent issues, ML/TF risks, and their mitigation, for clarification of the relevant requirements of the regulators, for professional development of employees of the supervised entities, and on other relevant topics are carried out on an ongoing basis. Employees of the supervisors, the FIU, and other concerned ministries and agencies are involved in these activities. These facts indicate significant efforts of the Republic of Uzbekistan to promote a clear understanding by the private sector of its AML/CFT obligations and ML/TF risks.

Financial Sector

1062. The country has demonstrated effective approaches to informing the private sector about the AML/CFT requirements and related risks. Methodological recommendations and guidelines are periodically sent to the sectors, and a large number of training events are held on various urgent topics, which, in particular, are related to the identified ML/TF threats, risks, and typologies.

1063. The CB takes a comprehensive approach to the training of its supervised entities on an ongoing basis. For the rest FIs, AML/CFT training is regularly conducted by the FIU, supervisors, the Leasing Association, and commodity exchanges, which evidences active work in this area.

Table 3.17. Communication of supervisors with FIs in 2016–2020

	2016		2017		2018		
	Guidelines and recommend ations	Work shops	Guidelines and recommenda tions	Work shops	Guidelines and recommenda tions	Risks	Work shops
Commercial banks	0	7	1	28	0	1	19
Microcredit institutions	0	1	0	2	1	0	3
Insurers and insurance brokers	2	1	1	1	3		1
Professional securities market participants	0		0		0		
Exchange members	0	2	0	3	0		1
Postal operators	5	7	3	11	3	1	9
Leasing services providers	0	0	0	0	0	0	0
Organizations conducting money remittances, payments and settlements	0	0	0	0	0	0	0
Pawnshops	0	1	0	2	1	0	3
VASPs	0	0	0	0	0	0	0
Total	7	19	5	47	8	2	36

	2019				2020			
	Guidelines and recommen dations	Trends and typologi es	Risks	Work shops	Guidelines and recommen dations	Trends and typologi es	Risks	Work shops
Commercial banks	8	4	1	18	11		1	12
Microcredit institutions	1	1	1	3	1		1	4
Insurers and insurance brokers	2			1	2			1
Professional securities market participants	0			4	20	0	0	10
Exchange members	0			1	0			1
Postal operators	6		1	6	5		1	9
Leasing services providers	0	0	0	0	0			
Organizations conducting money remittances, payments and settlements	0	0	0	0	0	0	0	0
Pawnshops	1	1	1	3	1		1	4
VASPs	0	0	0	0	0	1	0	0
Total	18	6	4	36	40	1	4	41

Banking Sector

1064. In 2016–2020, 84 AML/CFT workshops/training were organized for the employees responsible for AML/CFT internal control, and 5,741 employees participated in them. Also, in 2019–20, 11 AML/CFT workshops were organized for front office staff and auditors of commercial banks, and 643 participated in them.

1065. The main topics of the workshops and trainings: analysis of the main violations identified during inspections; enhancing mechanisms for combating economic crimes; recent changes to the internal control rules; the results of the sectoral risk assessment.

1066. In order to notify banks about the existing risks, typologies, schemes, and higher-risk transactions, the CB issued 4 letters in 2018, 18 in 2019, 11 in 2020, and 4 in the first half of 2020. The topics of the letters cover a wide range of urgent AML/CFT issues related to the identified vulnerabilities and risks and urgent issues of the sector.

Payment Institutions

1067. The CB has developed recommendations (common approaches) for regulating electronic payment systems in order to prevent their misuse for ML/TF. Since the supervisory regime has been implemented not so long ago, in 2020 2 workshops were conducted for payment institutions and payment system operators.

Exchange Trading Sector

1068. Workshops and training courses are held to support understanding of the risks. Thus, in 2016 2 workshops and 1 training course were held, in 2017 – 3 workshops, 2018 – 1 workshop, 2019 – 1 workshop and in 2020 – 1 webinar and 1 training course.

1069. Before granting access to exchange trading, the exchanges conduct tests for all traders with questions about the ICR and give instructions to persons responsible for compliance with the AML/CFT-related ICR.

1070. The staff of the Antimonopoly Committee and commodity exchanges took part in workshops organized by the FIU in cooperation with the International Training and Methodology Centre for Financial Monitoring (ITMCFM) via video conferencing on various AML/CFT topics. Also, the FIU together with experts from the World Bank organized a workshop on September 23-25, 2019 on the methodology of the World Bank for assessing risks and vulnerabilities of sectors.

1071. In 2019–2021, 13 recommendation materials were prepared and distributed, including:

- A letter to the exchanges suggesting the implementation of the electronic questionnaire survey in the test mode. But due to the complexity of the questionnaire itself, the implementation was postponed until making changes to the ICR;
- On publishing NOR 2019 and communicating its results to the exchange members;
- On revising financial sanctions against members of stock exchanges that violate the ICR;
- On elaborating freezing powers for exchange members.

1072. It is worth noting that banks, in addition to banking activities, carry out the activities of professional securities market participants and leasing activities. In addition, leasing activities are also carried out by microfinance organisations. It is therefore recommended to consider the possibility of organising an inter-agency exchange between the Ministry of Finance and the Central Bank regarding the identification of suspicious securities transactions by banks and leasing activities by banks and microcredit organisations.

VASPs

1073. In 2020, a working meeting was held with representatives of the only licensed crypto exchange that has not started operation. The purpose of the meeting was to clarify the ML/TF risks and AML/CFT/CPF responsibilities.

DNFBPs

1074. The supervisors exercise control and supervision jointly with the DCEC, which provides them with information on the existence of personal accounts (through which the lists are communicated) and the submitted reports. Also, the DCEC actively participates in awareness-raising work aimed at increasing the level of knowledge and law-abidingness of DNFBPs in the field of AML/CFT.

1075. All DNFBPs regularly undergo training organized by the supervisors and the DCEC. For example, in 2020, the DCEC conducted 8 workshops for different DNFBP sectors and supervisors, 8 in 2019, 8 in 2018, and 6 in 2017. Real estate agents, lawyers, notaries, and auditors undergo periodic professional development, which also includes AML/CFT issues.

1076. According to the presented protocols of training activities, they were aimed at a general understanding of the AML/CFT/CPF risks and the involvement of entities in the anti-money laundering system. At the same time, due to the lack of supervisory measures in most sectors and the complete absence of the facts of the application of sanctions for non-compliance with the AML/CFT requirements, the supervisors cannot ensure full understanding by the sectors of their responsibilities in this area. This is confirmed, first of all, by the absence of STRs from DNFBP sectors, and poor understanding of CDD procedures by the DPMS, real estate (for more details, see the analysis of IO.4).

1077. In order to increase supervised organizations' understanding of the threats and consequences of ML/TF and the importance of STR filing, the Ministry of Finance approved and posted on the website the Recommendations on the Application of the NRA Results (Protocol No. 2 of February 6, 2020), which include:

- typical indicators of the "Corruptionist" financial profile (cl. 4 of the Recommendations approved by Protocol No. 2 of February 06, 2020);
- negative consequences for the organizations involved in ML/FT (cl. 7 of the Recommendation approved by Protocol No. 2 of February 6, 2020).

1078. Moreover, the Ministry of Finance approved and agreed with the DCEC the Methodology for Assessing ML/TF Risks in the Activities of Audit Organizations, dated September 17, 2018.

1079. In order to increase the level of understanding of risks by the supervisors, and jointly with the DCEC, training events for representatives of the sectors are held and typologies of illegal activities, primarily predicate offenses are communicated. There is a practice of communicating various recommendations and guidelines to the sector participants, but these facts are sporadic. For example, information was communicated to the DPMS sector only in 2018, and the SRA report was communicated in 2020.

1080. Various guidelines and recommendations on the implementation of the AML/CFT requirements, as well as information on risks and typologies, are annually brought to the attention of the sector of notaries and lawyers, and auditors.

1081. Such information has not been separately communicated to the real estate sectors, except as part of ongoing workshops and refresher courses. In this context, it is important to note that real estate agents and auditors are required to undergo annual training, which covers, inter alia, AML/CFT issues.

1082. It is necessary to assess the significant effectiveness of conducting such training events and communicating methodological recommendations to all DNFBP sectors since due to the lack of full control over the implementation of the AML/CFT requirements, the assessors believe that it is through this work the supervised entities have an understanding of AML/CFT risks and responsibilities to mitigate them.

Overall conclusion on IO.3

1083. The CB introduced in all supervised sectors (banking, NBCIs, payment organizations) a risk-based approach in supervisory activities, which ensures the ranking of entities by the level of risk and application of supervision mechanisms corresponding to identified risks. Active remote monitoring and inspection checks are also in place. Considering the specifics of the postal transfer sector, supervision and inspections are carried out on a continuous basis and necessarily include AML/CFT elements. In the securities and insurance sectors, AML/CFT supervision is carried out as part of the

general prudential supervision without the RBA elements. In the sector of commodity exchanges the country demonstrated the process of transition to the RBA in the supervision. Considering the resources of regulators, the current supervision corresponds to the risks of the sector. The NAPM is active in suppressing illegal activities in the field of virtual assets, as there were no reporting entities at the time of the on-site mission. Due to the actual absence of AML/CFT compliance controls and the lack of sanctions for violations of AML/CFT requirements, the performance in achieving the IO3 in terms of DNFBPs is significantly lower compared to the financial sector.

1084. Despite the fact that at the time of the assessment the risk-based approach was not actually applied in the DNFBP sectors, the Republic of Uzbekistan is making efforts to implement it in its supervisory activities. This is primarily driven by the development of electronic monitoring systems and the adoption of legislative acts, which directly set out the requirements for AML/CFT supervision using the risk-based approach.

1085. Considering the weight and importance of the FI and DNFBP sectors, the experts assess the efforts of the Republic of Uzbekistan in implementing the risk-based approach in AML/CFT supervision and the overall system of AML/CFT supervision as moderate.

1086. **The Republic of Uzbekistan is rated as having a moderate level of effectiveness for IO.3.**

CHAPTER 7. LEGAL PERSONS AND ARRANGEMENTS

Key Findings and Recommended Actions

Key findings

1. Information on the creation and categories of legal persons in Uzbekistan, as well as the Single State Register of Business Entities (SSRBE) are publicly available. The legislation does not specify a body responsible for verifying the authenticity of the information submitted at the stage of state registration, as well as ensuring the accuracy and reliability of the information in the SSRBE. However, in practice, Public Services Centers (PSC) carry out such work. The most common type of legal persons in the country is LLC.
2. Legal arrangements in the sense of how this term is used in the FATF Recommendations cannot be created in Uzbekistan. Uzbekistan is not a member of the Hague Convention of 1 July 1985 on the Law Applicable to Trusts. The legislation provides for a relationship between foreign trusts and residents to generate income for the benefit of the settlor. At the time of the on-site mission, there were no relationships between residents and foreign trusts.
3. NRA was conducted to assess vulnerabilities and the extent to which legal persons could be used for ML/TF purposes. The NRA covered all known categories of legal persons. The competent authorities' understanding of the vulnerabilities of legal persons varies. The greatest is demonstrated by LEAs and some supervisory authorities. According to the NRA, LLCs are most often used for illegal purposes, including ML. There were no cases known (or identified) of misusing legal persons for TF purposes. NRA examined the role of professional service providers. Independent accountants and lawyers are not involved in the national AML/CFT system. The sector of professional accounting and legal service providers is not fully explored.
4. Conditions have been established to mitigate the misuse of legal persons. Special attention is given to ensuring the accuracy of basic information and BO data. Activities of legal persons are inspected and financial sanctions are applied. Legal acts are being modernized. LEAs successfully apply criminal laws and prevent the misuse of legal persons. “Dormant companies” are identified and liquidated. The share of non-cash payments between legal persons prevails. The legislation does not provide for the issue and circulation of bearer shares. The PSC denies registration of a legal person in case of providing incorrect information, banks deny carrying out transactions and establishing business relations if it is not possible to conduct CDD. STC imposes sanctions for failure to provide information on changes.
5. FIs and DNFBPs are obliged to conduct CDD when residents apply for services to carry out operations with a party of a foreign trust and theoretically are able to prevent the violation of the law. This can only be affected by the difference in understanding of their responsibilities by FIs (except for banks) and DNFBPs. Considering that there were no known cases of relationships between foreign trusts and residents at the time of the on-site mission assessors made their conclusions about the effectiveness of practical measures based only on theoretical judgments.
6. The main source of basic information and BO data with regard to all categories of legal persons in the country is the SSRBE. Additional sources are the information databases of other government agencies, as well as data collected by FIs and DNFBPs in the course of CDD. Some banks have their own databases on BO. DNFBPs do not have such databases. The greatest understanding of the need and procedures for identifying BO was demonstrated by FIs and some DNFBPs. Competent authorities have unconditional access to the basic information and BO data of legal persons created in the country and positively assess the quality of information from these sources. In some cases, it may take longer to obtain similar data with regard to foreign legal persons.
7. There are no sanctions to legal persons for providing inaccurate or unreliable information when registering. Sanctions are applied for failure to provide data in case of changes in the registration data of a legal person. Sanctions for failure to comply with requirements to keep and provide basic information about legal persons and BO, as well as limited measures in relation

to some DNFBPs for failure to collect such data, are considered by assessors to be insufficiently dissuasive.

Recommended actions

1. To increase the level of understanding of the vulnerabilities of legal persons among those supervisory bodies that are less aware of it. These supervisory bodies should ensure an appropriate level of understanding among their supervised entities. To continue similar work among FIs and DNFBPs on a regular basis. To continue assessment of vulnerabilities, focusing on the study of the most typical ones with respect to specific types of legal persons that may be created in the near future, or their activities. To explore the market of professional service providers (accountants, lawyers), to assess the vulnerabilities of their possible use for illegal purposes. To extend the AML/CFT law to independent accountants and lawyers and thereby ensure their direct involvement in the national anti-money laundering system.
2. At the legislative level assign the PSA with a) the obligation to verify the authenticity of information and documents provided for state registration and re-registration; b) the obligation to ensure the accuracy and compliance of the information provided with the law; c) the obligation to continuously monitor and ensure the accuracy and reliability of data in the SSRBE. PSA should update information on the BO of all legal persons created in Uzbekistan at one time, and continue this on a systematic basis.
3. To implement among all DNFBPs the practice of collecting and keeping data on BO, as well as updating these data. To ensure that all DNFBPs, especially those that do not understand how to identify BO (except for notaries, advocates, and auditors), get this understanding and are able to do so. To ensure that FIs and DNFBPs continue to collect basic information and BO data both when establishing a business relationship and in the course of such a relationship. To develop a specific Guideline or to include procedures for identifying BO in the ICRs for DNFBPs. To ensure that FIs and DNFBPs regularly monitor their relationships with legal persons and update their BO data. FI to continue applying the practice of denying operations of legal persons and keep statistics. Similar work should be carried out by DNFBPs.
4. To ensure that FIs and DNFBPs report discrepancies in the data, including beneficial ownership, provided by their clients - legal persons to competent authorities, primarily those registering when establishing a business relationship and in the course of such relationship. This will help cross-check the data and thereby continuously update and keep the basic information and information about the BO in the SSRBE up to date. To use ongoing supervision mechanisms and other methods to continue ensuring timely access by competent authorities to information (if available) on the relationship between foreign trusts and residents as well as legal arrangements.
5. To amend the current legislation to allow the PSA appling sanctions against applicants for providing inaccurate information during registration, and, if possible, to toughen these sanctions. Introduce a requirement in the current legislation to impose penalties on individuals for failing to provide information about BO or providing false information. Provide such measures in the relevant law or other law in an explicit form. To continue implementing measures to prevent the provision of inaccurate information in the registration of legal persons, using the existing mechanisms before changes to the legislation come into force.

1087. This chapter reviews and evaluates the achievement of Immediate Outcome 5. The recommendations relevant to evaluating effectiveness under this section are 24 and 25, as well as elements of Recommendations 1, 10, 37, and 40[67].

[67] 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.

Immediate Outcome 5 (Legal Persons and Arrangements)

1088. As of July 1, 2021, 615,109 legal persons in all organizational and legal forms were registered in Uzbekistan including 373,713 between 2017 and 2021. The registration of such a large number of legal persons in recent years was explained by the competent authorities by simplifying state registration, improving currency policy, reducing the tax burden, and generally creating a favorable environment for doing business. LLCs are the most common type of legal persons in the country (more than 45% of the total number of registered). The predominant share of legal persons is held by residents (less than 1% by enterprises with foreign capital). Almost all categories of legal persons are engaged in commercial activities. Companies are considered inactive if they do not carry out financial activities for 9 months. Tax authorities identify and liquidate "dormant companies". From 2016 to the first half of 2021 more than 46 thousand companies were liquidated.

1089. Legal persons inform state authorities about changes in charter documents, founders and composition of their shares, beneficiaries, as well as all other changes within 30 days. 30 days is the maximum period. In practice, it usually happens within 10 days.

Table 5.1. Information about legal persons registered in the Republic of Uzbekistan in the period from 2016 to 2020

№	Forms of incorporation of legal persons	2016	2017	2018	2019	2020
1	Private enterprise	6245	4834	8384	18664	12425
2	Family business	2863	2266	4432	13054	17958
3	Farming enterprise	48727	13072	18770	8904	9939
4	Dehqan farm	2362	828	882	1287	1033
5	Limited liability companies	21893	17007	35699	60693	61664
6	Supplementary liability company	0	29	30	30	9
7	Joint stock companies	17	5	16	23	15
8	Unitary enterprise	91	250	308	281	156
9	State unitary enterprise	27	163	154	66	23
10	Production cooperative	5	71	28	143	1110
11	Unlimited partnership	4	2	1	3	1
12	Limited partnership	2	0	0	1	3
13	Total	82236	38527	68704	103149	104336
14	Foreign invested enterprises	715	284	830	971	595
15	Number of legal persons excluded from the Register [68]	25432	22066	15713	15777	7887

Public availability of information on the creation and types of legal persons and arrangements

1090. Information on the creation and organizational-legal forms of legal persons in Uzbekistan, as well as the Single State Register of Business Entities (SSRBE)[69] are publicly available. The list of types of legal persons is given in Table 5.1. Registration of legal persons is carried out by the Public Service Centers (PSC) of the Public Service Agency (PSA) under the MJ. Detailed information about the registration procedure can be found on the PSA website[70]. The information contained in the SSRBE is kept permanently on the basis of the principle of "accumulation" and shall not be deleted. The legislation does not specify the body responsible for verifying the authenticity of information and documents submitted for state registration, as well as for ensuring the accuracy and reliability of the data contained in the SSRBE. However, in practice, this is the responsibility of the PSC.

[68] Bankruptcy; voluntary liquidation; liquidation due to no financial and economic activities from the moment of state registration; termination of activities due to reorganization, merger or acquisition, etc.
[69] https://fo.birdarcha.uz/pub/search (the information in the registry is given in the state language)
[70] https://davxizmat.uz/

1091. Legal arrangements in the sense how this term is used in the FATF Recommendations cannot be created in Uzbekistan. Uzbekistan is not a member of the Hague Convention of 1 July 1985 on the Law Applicable to Trusts and their Recognition. At the same time, the legislation provides for relationships between foreign trusts and residents to receive income for the benefit of the settlor. The settlor of the foreign trust is registered with the tax authorities and reports to the STC on the participation in the trust relationship. There are no barriers to obtaining information from a resident participating in a foreign trust. At the time of the on-site mission, there were no relationships between residents and foreign trusts.

Identification, assessment and understanding of ML/TF risks and vulnerabilities of legal persons

1092. Competent authorities have demonstrated a good understanding of how legal persons can be used for ML purposes. However, the extent of this understanding varies among government agencies. The assessment of vulnerabilities and the extent to which legal persons could be (are) used for ML/TF purposes was conducted in the course of the NRA. There were no cases known (or identified) of misusing legal persons for TF purposes at the time of the on-site mission. In the course of the NRA, the practical specifics of the activities of legal persons were examined, and the materials of criminal cases and the results of financial investigations involving legal persons were studied. The reasons and conditions contributing to the commission of crimes in which legal persons were involved have been analyzed.

1093. According to the NRA, LLCs are most often used for illegal purposes, including ML, due to the simplicity of their registration, expressed in its declarative nature; an extensive range of activities that can be carried out by LLCs; liberalization of currency policy; low requirements for the size of the authorized capital; and simplified taxation. The most typical use of LLCs for illegal purposes is cash-out. Different mechanisms can be used for this purpose. For example, transferring money from the LLC account(s) to individuals for fictitious services or by granting a financial loan in favor of a legal or natural person. The LEAs also noted the following cases of legal persons being used for criminal purposes: a) as front companies to conceal illegal activities; b) to conceal BO through front persons; c) for tax evasion. The NRA results in terms of the above-mentioned vulnerabilities of LLCs correlate with examples of criminal cases of money laundering.

Case Study 5.1. (Using a legal person to illegally cash out funds)

FIU analyzed over 200 (two hundred) transactions of LLC "A" and found that in 2018, funds of over 17 billion UZS (USD 2.5 million) received to LLC's account from construction companies were transferred to 15 IEs for allegedly rendered services. FIU found that the IEs were front men[71]. The money received on their accounts was transferred to the cards of other IEs, also front men, and cashed out by the beneficiary of LLC "A" under powers of attorney. The BO of LLC A was detected in the course of the ORM on the basis of the testimony of the front men. FIU initiated criminal proceedings against the BO of LLC "A" and the defendants for embezzlement of budgetary funds, pseudo-entrepreneurship, tax evasion, violation of trade rules and legalization of criminal proceeds. The court found BO "A" and the defendants guilty of the abovementioned crimes and sentenced them to 3 years in prison for pseudo-entrepreneurship, 8 years in prison with deprivation of the right to hold managerial and materially responsible positions for 3 years for theft by embezzlement, 4 years in prison for tax evasion, 6 months in custody for trade or services violation, and 7 years in prison for money laundering. The cumulative sentence imposed on BO of LLC "A" was 11 years in prison with deprivation of the right to hold certain positions for 3 years and a fine of 121,638,000 UZS (USD 14,700,000), to be paid to the state.

[71] The term "front men" is not regulated in the Uzbek legislation. It is used by LEAs in investigations as a verbal turnover to refer to persons providing paid services (for example, in the role of a fictitious director or owner). Predominantly, the role of "front men" is played by socially vulnerable groups or close relatives.

1094. The NRA also examined the role of "intermediaries" in the creation and management of legal persons. According to the report, audit organizations provide professional accounting services to legal persons, which are limited to the development of accounting policies and chart of accounts, preparation of financial calculations and payroll statements, and preparation of financial reporting forms. According to the NRA, the services provided by auditors are not related to transactions with cash or other property. The NRA conclusions in this part were confirmed by representatives of audit companies during the meetings.

1095. Professional services to legal persons in Uzbekistan are also provided by advocates, legal advisors[72] and accountants. The advocates provide services[73] on the basis of license. Legal advising is provided by professional lawyers who are on the staff of organizations of legal consultants, a register of which is maintained by the MJ. These services are provided on a contractual basis to individuals and legal persons. Accountants provide accounting services in companies on the basis of employment contracts, thereby becoming staff members of the organization. The activities of independent accountants, who are not on the staff of the companies, at the time of the on-site mission were not detected. Financial transactions are performed by legal persons themselves. Professional services provided by advocates, lawyers and accountants are limited to the preparation of documents and their support. No cases of providing legal and accounting services outside of the Uzbek legislation in force at the time of the on-site mission were identified by the competent authorities.

1096. Despite the clarity in terms of services provided by advocates, assessors believe that the role of independent accountants and legal advisors requires greater understanding by the competent authorities. The assessors are inclined to believe that these entities are not adequately supervised, and that it is unclear whether those who may provide or are already providing professional services to legal persons, including for illegal purposes, are identified among them. These conclusions are made on the basis of data obtained from representatives of audit companies and public sources[74]. Independent accountants and lawyers providing professional accounting and legal services are not involved in the national AML/CFT system, but they are subject to the same requirements as others under current legislation. This situation, in the assessors' opinion, may mean that this sector has not yet been sufficiently explored in Uzbekistan. Assessors believe that the lack of attention to the professional services sector may include vulnerabilities to its illegal use. No evidence to the contrary has been provided.

1097. LEAs; supervisors of banks, micro-credit organizations; insurance companies; professional securities market participants; exchanges; postal operators; payment systems; pawnshops; notaries and advocates; and auditors demonstrated a good understanding of the vulnerabilities and extent to which legal persons can be misused, and were able to confirm the NRA's findings. Representatives of the individual supervisory agencies responsible for regulating dealers in precious metals and dealers in precious stones, lotteries, and real estate agents did not demonstrate a good understanding of the vulnerabilities of legal persons and the likelihood of their misuse.

Mitigating measures to prevent the misuse of legal persons and arrangements

1098. In Uzbekistan significant measures are taken to prevent the misuse of legal persons and arrangements for ML/TF purposes. At the same time, it should be noted that the measures in relation to legal arrangements have been evaluated by assessors on the basis of theoretical judgments. The measures correlate with the vulnerabilities identified in the NRA and include, but are not limited to ensuring the accuracy and reliability of basic information and BO data of legal persons; inspections of legal persons; LEAs measures; modernization of legal acts establishing obligations to provide data on a legal person and BO before and after registration and to report changes in it; interaction of competent

[72] A natural person who has a higher legal education and at least two years of experience in the legal profession and is on the staff of the organization of legal advisors (in accordance with Annex 1 to the Cabinet of Ministers Decree of August 17, 2018 № 675).
[73] See para 959.
[74] https://favorit-legal.uz/oformleniye-imushchestva; https://legalact.uz/ru/services.

authorities with reporting entities to prevent their use in illegal operations in which legal persons are involved; denials of state registration and carrying out banking operations. Legal persons use non-cash payments, but cash payments are also not prohibited. The predominance of non-cash payments, according to assessors, reduces the vulnerability of the use of legal persons for illegal purposes. The assessors' position correlates with the NRA results. The Uzbek legislation does not envisage the issuance and circulation of bearer shares, only registered shares are permitted. Issue and circulation of bearer securities were possible until 2009. (for details see analysis under Recommendation 24).

Ensuring the accuracy and reliability of basic information and BO data in the SSRBE

1099. The results of the authorities' efforts to ensure the accuracy and reliability of basic information and BO data are evaluated by assessors as effective. However, these measures may have a greater effect if the applicants will be sanctioned for providing unreliable, inaccurate, as well as misleading information at the stage of state registration. The PSA should update BO data for all legal persons and do it on a systematic basis.

Registration authorities

1100. Competent authorities consider ensuring the accuracy and reliability of basic information and BO data in the SSRBE, databases of government agencies, and the private sector as the first line of defense to prevent the misuse of legal persons. In order to achieve the above objective, the process of state registration of legal persons and the entry of accurate and reliable data in the SSRBE is of paramount importance. Registration of legal persons is declarative in nature and is made at the time of application to the PSC. Registration takes from 30 minutes to one day[75] and is carried out in two stages[76] (application and founding documents). Applications can also be submitted remotely. In this case, applicants first receive an e-digital signature[77].

1101. Applicants are responsible for the authenticity, accuracy, and misrepresentation of information submitted to the PSC. According to the law (paragraph 53 of the Regulations on the procedure of state registration approved by the Decree of the CM-66 of 09.02.2017), registration authorities do not verify the authenticity of information and documents submitted for state registration, re-registration, and do not bear responsibility for the accuracy and inconsistency with the law. At the same time, during the meetings representatives of the PSA noted that, in practice, PSC verifies the information provided at the stage of state registration by the founders of legal persons. The assessors were able to verify this because the PSC provided supporting materials[78], including classified ones.

1102. Only founders or authorized persons may apply for state registration of a legal person. If a company to be registered has several founders, the applicant provides a notarized power of attorney. When registering a legal person through a third party, the participation of one of the founders (if more than one) is required, who must act on the basis of a power of attorney or the consent of the founders, drawn up in accordance with the law. Non-residents apply to the PSC for registration only in an unsolicited manner. They are subject to measures similar to those established for residents. When accepting applicants for service, employees of the PSC first of all check the applicant's identity documents (passport, another document (military ID card, driving license).

1103. The PSC verifies the authenticity of the applicant's identity documents through Unified Identification System (UIS) users of the electronic government of the Republic of Uzbekistan[79]. The registration system of legal persons of the PSC is connected to the data of the UIS. To receive interactive state services, including registration of legal persons, all users must pass authorization and receive a login and password in the UIS. To get a login and password, user identification data must be entered, which

[75] Until 2017, 2 to 7 days.
[76] Until 2017 in six phases.
[77] https://my.gov.uz/ru/service/357
[78] Screenshots of the system of registration of business entities, documents regulating the rights and duties of employees of the PSC in the registration and verification of information, internal orders to verify the identity of applicants with data from the List of persons associated with terrorist activities were presented.
[79] The state information system that provides identification of individuals and legal persons, as well as authorized access of officials of relevant ministries and departments to information systems and databases during interdepartmental electronic interaction - https://id.egov.uz/?client_id=fo_birdarcha&token_id.

will have to coincide with the data of other government agencies, tied to the electronic government, for example, the MIA. Thus, in order to get to the process of registration of a legal person the applicants pass through several stages of identification and identity verification. When checking the non-resident founder's passport, the border crossing marks are checked. It is for this purpose that a PSC employee requests the original passport in the personal presence of the person. In this case, the PSC relies on border control systems and verification of the identity of the applicant (passport) when crossing the state border.

1104. The PSC also conducts a comprehensive review of the information provided by the applicant to verify its compliance with the list, including the BO data. The PSC relies on the beneficial ownership information provided by the applicant. When re-registering a legal person, the registering authority uses the BO data provided by the CB. This information is integrated into the work program of the PSC staff and is used regularly. As of April 2021, all legal persons are required to provide BO data at the registration stage by entering this information in the questionnaire form[80]. Despite the relatively recent introduction of the requirement in the legislation to provide information on the BO, before that, all legal persons without exception provided information on their founders and their shares in the authorized capital. Thus, all interested parties, including the competent authorities, could see the ownership structure and division of shares in the organization.

1105. The PSC also verifies the documents certifying the authority of the person acting on the basis of the power of attorney. If one of the founders is a foreign legal person, the PSC requests an extract from the Commercial Register of the country in which the legal person was founded (legalized, translated into the national language, and notarized). The PSC also checks the personal data of all applicants against the List of terrorists. The list is an integral part of the automated system of business registration. The assessors were provided with supporting materials, which indicate the presence of the above functionality in the working program of the PSC employees. In case of a match, registration is suspended and the Central Office is immediately notified, the data is then transferred to the FIU. There were no cases of matches registered at the time of the on-site mission.

1106. The PSC, among other things, checks applicants for their presence on the wanted list and also checks applicants who are legal persons through a blacklist of business names[81]. Only if the data submitted by the applicant meets the registration requirements, information about the legal person is entered into the SSRBE, and the registration is completed.

1107. The documents kept by the registering authority and the SSRBE take precedence in case of discrepancies with the data in the founding documents and the organization's documents in general. The information contained in the SSRBE is kept permanently and even after the liquidation of the legal person is not deleted from the PSA servers.

1108. Resident founders of legal persons can open a bank account in national and foreign currency in the process of state registration both in person at the PSC and remotely (if the conditions for remote identification are available). To do this, the applicant fills out an application for remote account opening and chooses from a list of 1 of 863 branches of commercial banks. Then completes the necessary information, as well as accepts the terms of the offer of a bank account placed in the PSC System. After that, the executed application together with founding documents and information on the state registration of the legal person are sent through an automated system to the selected branch of a bank. The bank account is opened by accepting the offer of a contract of bank account, placed in

---

[80] In order to verify the effectiveness of the practice introduced to collect beneficial ownership information PSA conducted a control check of 4114 legal persons registered in the period from April 21 to May 1, 2021. According to the results of the check all legal persons without exception indicated the BO. In most cases the founder was specified as BO, but in 328 cases different information about the founders and beneficiaries was specified. In addition to residents, citizens of Turkey, Iran, Afghanistan, Azerbaijan, Russia, Kazakhstan and New Zealand were also listed as BO. The assessors positively evaluate the control inspection and the results achieved as a result of it.

[81] The Law "On firm names" September 18, 2006, № ZRU-51 establishes the designations which should not be in the name of the registered organization. PSC, based on the categories specified in the list, select the words or parts of words that are prohibited for registration. If there is a full match with the prohibited designations, the system goes into red alert and refuses to accept that name. A firm name, among other things, must not contain denominations that are identical or similar to the extent of their confusion with the firm names, previously registered or applied for registration in the Republic of Uzbekistan in the name of another legal person; with trademarks (service marks), previously registered or applied for registration in the Republic of Uzbekistan in the name of another person.

the System. Then the founder of the legal person applies to the bank, where the account is opened and conducts bank operations. The bank conducts CDD procedures before carrying out operations on the account.

1109. Non-resident founders must apply to the bank on their own and fill out an application to open an account there. The bank conducts CDD when establishing a business relationship with such a non-resident customer.

1110. According to the Decree of the President of Uzbekistan from 23.03.2021 #UP-6191 "On additional measures to further create favorable conditions for the population and entrepreneurs in the use of public services, reducing bureaucratic barriers in this direction" from July 1, 2021 registration of taxpayers and their registration is carried out only with a personal identification number of a natural person (PINNP).

1111. Persons who have not received PINNP will not be able to register a legal person, the same applies to foreign founders. In order to register a legal person, foreign founders need to apply with their passport to the internal affairs authorities with an application for the issuance of a PINNP. Only after receiving the number, the founders can apply to the PSC for registration of the legal person. Providing a power of attorney from the foreign founder is not the basis for registration. A foreign founder, who has issued a power of attorney, must first obtain a PINNP to have all information about him displayed in the identification system. Thus, the identification of all users, without exception, is carried out by the UIS.

Tax authorities

1112. An equally important role in ensuring the accuracy and reliability of basic information and BO data of legal persons belongs to the tax authorities, as well as FIs (banks). When registering a legal person, their registration with the tax authorities is carried out at the same time. Data on the new company gets to the appropriate divisions of the STC and is highlighted in the database as an object requiring attention. The inspection starts within 10 days after the registration. Tax authorities have enough resources to conduct such inspections.

1113. Thus, based on the calculation of 248 working days in 2020, the number of registered legal persons – is 104 thousand and the number of employees is 2 thousand, on average, for one working day per employee falls 104.000/2.000/248 = 0.21 legal persons, or, in other words, an average of 5 working days (week) to check one legal person. Thus, in one year each employee of the tax authorities checks 52 legal persons, including the fact that they indicated accurate and reliable information at the stage of state registration. In the course of inspections, all data, without exception, are comprehensively checked. Checks are made both in-person and remotely. In case of in-person inspection, an employee of the tax authority visits the place of registration and checks all the information provided by the applicant during the registration. Tax authorities also check whether several different companies are registered in the founder's name and whether the same address is used by several entities.

Financial institutions

1114. Banks conduct CDD and check the data indicated by the customer for consistency with the SSRBE. If inaccuracies are detected, the bank denies service to the customer and sends it to the PSC for re-registration. Banks identify the BO of their clients by analyzing the data on the founders and ownership structure. If as a result of the measures taken doubts arise as to whether the person having the controlling interest is the BO, the bank may confirm or deny the data by analyzing the banking transactions performed by the client. This information is periodically updated according to the customer's risk level. For more information on the detection of BO by banks, see the analysis on the achievement of IO.4 in the section "Compliance with CDD requirements and record/document keeping". The CB organized a one-time submission by banks of the BO data of their customers. The new data has been transmitted by the CB to the PSA. PSC actively use them to reconcile the BO information provided by applicants at the stage of re-registration.

Preventive measures taken by the competent authorities to ensure that legal persons and arrangements

are not used for illegal purposes

1115. In order to combat the illegal use of legal persons, in addition to measures to ensure the accuracy and reliability of data a number of measures of a preventive nature are taken in Uzbekistan. These measures include the use of criminal law against officials of legal persons, inspections by tax authorities to prevent illegal activities of enterprises, denials of state registration by the PSC and denials of service by the FI, sanctions for failure to provide information, and others. Assessors positively assess the existence of the measures taken, but also believe that these measures could be strengthened if administrative liability is applied to legal persons.

Enforcement of criminal law

1116. The FIU takes various measures to prevent the use of legal persons for illegal purposes. LEAs cooperate with the FIU, and joint investigative groups are established. Between 2016 and 2020 the FIU, as the main body responsible for investigating economic crimes, initiated and investigated 7,416 cases involving 8,522 legal persons. The investigations resulted in additional taxes of 4,834.9 billion UZS, or USD 791.7 million, and the imposition of financial sanctions totaling 2,216.4 billion UZS, or USD 385 million. All of the following cases and imposed penalties relate specifically to the misuse of legal persons under the following dispositions: suppression of the activities of shell companies; unlicensed activities; and violation of public procurement rules. Assessors believe that the measures taken by the LEAs are dissuasive and contribute to making the sector of legal persons less attractive to abusers.

Table 5.2. Information on revealed by the FIU offenses committed with the use of legal persons

Year	Criminal/administrative cases committed with the use of legal persons or connected with the activity of legal persons	Legal persons involved in criminal cases	Results of documentary checks of the activity of legal persons			
			Additionaliy charged taxes and fees (bln. UZS)	mln. USD	Fines imposed on legal persons (bln. UZS	mln. USD
2016	1 717	2 754	832,7	280,5	428,6	144,4
2017	1 266	1 595	801,0	155,8	515,2	100,2
2018	1 267	1 832	911,3	112,9	287,6	35,6
2019	1 471	1 111	1 043,5	117,9	484,8	54,8
2020	1 695	1 230	1 246,4	124,6	500,2	50,0
Total	7 416	8 522	4 834,9	791,7	2 216,4	385,0

1117. The FIU uses various methods to combat the illegal use of legal persons. One example of such work is the identification of the typology of the use of internet banking and tax reporting by shadow heads (BO) of legal persons for illegal purposes. The FIU has revealed that shadow heads register legal persons in the name of fictitious persons, and receive electronic keys for banking operations and tax reporting. Then an accountant is hired who sends tax returns on behalf of his clients, the front men. The FIU developed and implemented a mechanism to identify the shadow head of a legal person by establishing the approximate physical address from which connections were made to the data of companies (LLCs) via the internet. This result was achieved by deciphering the IP address of the computer used to access the internet. The mechanism has been brought to the attention of all the LEAs for use in their work.

Case Study 5.2. (Detection of shadow head of legal persons via IP address)

Citizen "Batir" in order to evade taxes, abusing the trust of "Sanat" and using his electronic key, registered three LLCs: "Service", "Contractor" and "Grocery". With the help of "Sanat" citizen "Batir" concluded an agreement with the bank "Trust us" for remote services and registered electronic keys with the tax

authorities for the submission of reports. An unreasonable increase in transactions on the accounts of these LLCs was the reason for the enhanced CDD. It was found out that the LLCs were not registered at their place of registration, and their managers did not have enough material resources and skills for conducting such large transactions. As a result of the inspection, the bank immediately suspended operations on the accounts of the LLC and sent an STR with the indication of the IP addresses from which requests for operations were sent to the FIU.

FIU established the identity of a citizen "Batir", who during the interview indicated that he gave electronic keys to a certain "Afruz" for a fee, but did not disclose any detailed information about him. FIU, according to the IP addresses received from the tax authorities, through which the electronic tax reports were provided, sent a request to the Special Center №XXXX. According to the data received, the approximate physical address from which all LLCs were connected to the internet, as well as information about the subscriber - internet user. In the course of the ORM, the office where the bank transactions were conducted was identified, as well as the identity of "Afruz", in whose name internet services were registered and the agreement on office lease was concluded. During the inspection of the office the electronic keys of LLC "Service", "Contractor", "Grocery" and "Own Business" were found.

An analysis of the banking transactions of Svoy Business LLC showed that a number of transfers were made from the above-mentioned LLCs for allegedly providing transportation services to Svoy Business LLC, which were subsequently transferred to Afruz's payment card in the form of dividends and spent on the purchase of a car. In his testimony, Afruz confessed to the crime and confirmed that he received income from illegal activities in the form of 2% of each debit turnover of LLC "Service", "Contractor" and "Grocery", which he subsequently transferred to his firm allegedly for transportation services and withdrew as profit for the purchase of the car. The FIU opened criminal cases for pseudo-entrepreneurship, tax evasion, trade violations and legalization of criminal proceeds. Batir and Afruz were convicted and sentenced to six years in prison, each to a fine of 116,500,000 UZS (USD 12,000).

Inspections and other activities of the STC

1118. The tax authorities, in order to prevent violations by legal persons, carry out inspections of their activities, which result in additional taxes, fines applied, and various amounts recovered to the state. STC has sufficient resources to check the activities of legal persons. More than 2,000 (two thousand) employees are allocated for this purpose.

1119. According to the results of the NRA STC introduced a risk-analysis system to assess the risks of tax violations. The system analyzes the data and gives a result on the degree of violation according to a point system. Business entities are then divided into three groups depending on the degree of risk: a) entities with increased risk; b) entities with average tax risk; c) entities with low risk. Assessors were not able to visit and see how the system of risk analysis functions, but the results of its use, demonstrated by the tax authorities during the meetings, demonstrated the consistency of the approach as a tool to respond to tax risks. In the analysis of risks are used indicators of suspicious activity in the actions of the legal person, 10 of which are devoted to determining the high risk of using legal persons in pseudo-entrepreneurship and fraud.

Table 5.5. Information about tax audits (sanctions are shown in billion soums).

№	Period	Total number of audits	Of which, in criminal matters	Taxes and payments charged additionally		Amount of implemented targeted financial sanctions		Amounts charged based on the audit results
				Number	Amount	Number	Amount	
1	2016	18 624	3 675	15 824	890,8	1 772	457,5	693,2
2	2017	15 131	1 876	13 935	767,2	1 072	352,6	469,7
3	2018	6 998	1 845	5 657	809,4	406	487,2	236,6
4	2019	5 356	1 567	4 234	906,4	382	402,0	178,6

5	2020	12 758	1 866	6 768	1 478,4	2 778	1 629,5	137,4

1120. In six months of using the risk-analysis system (as of June 16, 2021), 789 organizations engaged in "dubious" operations were detected, whose turnover totaled 12.4 trillion UZS (USD 1.2 billion) and unpaid VAT totaled 1.6 trillion UZS (USD 154 million). Tax control materials with respect to "dubious" organizations were sent to LEAs, criminal cases were initiated, additional taxes of 650 billion UZS (USD 61.3 million) were charged in 237 cases, and financial sanctions were applied for a total of 285.1 billion UZS (USD 26.9 million). STC representatives noted that the risk-analysis system facilitates the application of targeted measures, allowing for the effective allocation of human resources. Assessors positively assess the results of applying the risk analysis system and note their effectiveness.

1121. There is a joint Decree between the STC and FIU on the order of interaction on the prevention, detection, and suppression of violations and crimes in the tax sphere. In addition, there is a program for the implementation of a joint action plan to ensure the prevention of tax evasion, timely detection and elimination. The program, among other things, includes regular activities aimed at detecting and suppressing the activities of "shell companies" and "money-laundering offices". According to the STC, interagency agreements have also been signed with other LEAs. Representatives of the STC noted that the FIU regularly sends them various schemes of tax evasion, illegal cashing of funds, embezzlement of budget funds, and others. The tax authorities analyze illegal schemes and integrate them into their inspection plans and risk analysis system.

Case Study 5.3. (Cashing out money through notaries' execution writs)

FIU conducted an analysis of STRs and revealed transactions related to enforcement inscriptions of notaries in the amount of over 70 billion UZS (USD 6.8 million). It was found that within a short period of time the funds received on the accounts of 6 firms registered in the name of front men were transferred to a special account of the Bureau of Enforcement, as the latter had seized all outgoing transactions of the current accounts of these firms on the basis of notaries' writs of execution.

It was found that the companies acted as guarantors under the sham loan contracts through notary offices in the amount of 6-15 billion UZS (from USD 570 thousand to 1.4 million) for 6-10 days with the condition that 5% of the total amount of the contract for each day past due should be charged as a fine. Creditors were natural persons and debtors were founders and heads of companies. The incoming funds from the Bureau of Enforcement account were transferred to the bank cards of the alleged creditors as repayment of debts. The money was then cashed out by Citizen "C" (the bank of 6 companies) through the banks' cash desks by means of powers of attorney for the front men who acted as creditors.

During the investigation, the FIU sent a request to the tax authorities to conduct a field audit of 6 firms, as well as their counterparties. The inspection revealed violations and additional taxes and fees as well as financial sanctions of 20 billion UZS (1.93 million USD) were imposed. VAT credits were canceled against legal persons, counterparties that evaded taxes to cash out and transfer money into the "shadow" turnover. Based on the results of an inquest, including the materials of a field audit, the FIU opened criminal cases for pseudo-entrepreneurship, tax evasion and violation of the rules of trade or provision of services. Information messages were sent to the CB and the MJ to increase the attention of banks and notary bodies to certain types of suspicious operations and transactions. A court verdict found the heads of the firms and other defendants guilty and sentenced them to 3 years in prison for pseudo-entrepreneurship, 4 years in prison for tax evasion, and 6 months in custody for violating the rules of trade or services. Citizen C was sentenced to six years' imprisonment and a fine of 110,000,000 UZS (USD 12,500,000), the final fine being added to the state’s revenue.

International cooperation of STC

1122. STC exchanges data on legal persons, including BO. At the time of the on-site mission, 54 cooperation agreements between the STC and tax authorities of foreign countries were in force. A

list of the agreements is available on the STC website[82]. Between 2016 and 2019 STC neither received nor sent international requests for the exchange of basic information and on the BO of legal persons or other entities. The exchange of data on legal persons took place in 2020. The practice of the exchange of information on legal persons by the tax authorities of Uzbekistan with foreign state bodies is assessed positively by assessors. At the same time, assessors believe that the tax authorities could more often use international cooperation for the purpose of collecting data on BO.

Denials of state registration

1123. From 2016 to 2020, registration was denied in 8017 cases (see Table 5.3.). Assessors positively evaluate the use of denials as a tool to prevent dishonest businesses from entering the market. It serves as a barrier to their misuse for illegal purposes, including ML/TF.

Table 5.3. Information on denials of state registration of legal persons

No.	Reasons why legal persons were denied state registration	2016	2017	2018	2019	2020
1	Discrepancy between the submitted personal data and the information contained in the UIS	47	354	831	1167	1207
2	Submission of incomplete set of documents and/or information	96	76	248	355	701
3	Decision taken on approval (conclusion), amendments and/or additions to the constituent documents by a body with no relevant authorization by virtue of law and constituent documents*	89	0	229	406	533
4	Failure to submit documents in the manner prescribed by the law (upon re-registration)	0	0	0	101	28
5	Size of the authorized capital determined in the constituent documents below the minimum size**	48	75	354	507	281
6	Failure to submit documents in the state language, as well as their non-confirmation by the founders in the prescribed manner	37	0	88	0	0
Total		401	505	1768	2536	2807

** In cases of an increase in the size of the authorized capital, transfer of a share (contribution), reorganization.*
*** Stipulated for corporate entrepreneurs, for which the law establishes requirements for the size of the authorized capital for state registration, re-registration.*

Denials by banks to conduct operations

1124. The FIU regularly notifies the CB of the typologies of the use of banking services for illegal purposes, and the Bank brings these schemes to the attention of its reporting entities. The banks met during the on-site mission noted that they do not establish business relationships or refuse to conduct transactions with legal persons if there is no possibility to conduct CDD or otherwise verify the validity or legality of the transaction made through the bank. Two of the three banks with which on-site meetings were held noted that from 2017 to 2020 a total of 86 denials were made due to the impossibility of conducting CDD. The reasons for denials were the failure to provide documents requested under the law or the provision of false data; unusual behavior of the client when applying (order, petition); inconsistency of the client's operations with the type of activity carried out by his organization.

Case Study 5.4. (Bank's denial of an operation to a legal person)

In 2019, while analyzing the activities of its clients, the bank identified the organization "X" LLC, which made a large volume of transactions ~ USD 1 million in 2 weeks. Further examination revealed inconsistencies in the goods and services specified in the purposes of incoming and outgoing payments. For example, cash is received into the account for some goods, but payments are made for other goods. From the accounts of the enterprise money was transferred to different companies for food products, construction materials, etc. The company's current account was mainly used to receive money for household appliances, office equipment, bananas, and furniture, as well as financial aid and a loan.

[82] https://soliq.uz/page/xalqaro-hamkorlik

Enhanced CDD measures were taken with respect to "X" LLC and additional information was requested on the purpose of the client's transactions. The client did not provide any documents, on the basis of which the bank denied the transactions and terminated the relationship. The bank sent a report to the FIU.

Sanctions for failure to provide information about changes

1125. STC and PSA do not apply sanctions for providing inaccurate or unreliable information at the registration stage. Financial sanctions in the form of fines of ten (10) to fifteen (15) RSV are imposed on officials of organizations for failure to provide or providing false data on changes of address (location), bank details, or re-registration. This set of sanctions is seen by the STC as dissuasive, given the average wage[83] (2 877 700 UZS or USD 270). Nevertheless, assessors do not agree with this opinion and believe that these sanctions may not have a dissuasive effect if applied to dishonest persons, given the volume of their income. From 2016 to 2020, sanctions were applied only for failure to locate legal persons at their declared legal address.

Table 5.4: Offences related to absence of business entities at stated (postal) addresses identified by tax authorities and imposed fines (UZS mln)

TOTAL		Identified Offences Covered by CAO Art.176-2									
		2016		2017		2018		2019		2020	
Number	Amount	Number	Amount	Number	Amount	Number	Amount	Number	Amount	Number	Amount
982	2589,5	139	181,0	180	269,6	129	222,2	359	727,8	175	1188,9

Other measures

1126. According to the Decree of the President of Uzbekistan №UP-6098 of 30.10.2020. "On organizational measures to reduce the shadow economy and improve the efficiency of the tax authorities" the relevant Action Plan for its implementation was developed. During the meetings with the STC, it was noted that as a result of the Decree's implementation it was possible to achieve a 30% increase in revenues by "taking out of the shadow" income and the number of persons receiving income and paying taxes; reduction in the number of "shell companies". Assessors consider the results achieved through the implementation of the Decree as positive.

1127. In order to increase the transparency of the activities of legal persons a list of business entities that have abused the right to reduce the amount of VAT[84] has been compiled. There are two more resources to check the debt of counterparties[85], as well as to determine whether they are VAT payers or not, and thus eliminate the risk of tax violations[86].

Legal arrangements

1128. If a resident applies to the FI or DNFBP to conduct a banking transaction with a trustee of a foreign trust, the CDD will be applied. Thus, the FI and DNFBP will have information about the trust or other entity with respect to which the resident conducts the transaction and about the resident himself. However, what may affect this is the difference in the level of understanding of their responsibilities by the FIs and DNFBP. They are able to prevent violations of applicable law by residents or a party to a foreign trust. Unfortunately, due to the fact that at the time of the on-site mission there were no

[83] https://stat.uz/ru/press-tsentr/novosti-goskomstata/8980-srednemesyachnaya-nominal-naya-nachislennaya-zarabotnaya-plata-rabotnikov-predpriyatij-obladayushchikh-statusom-yuridicheskikh-lits-yanvar-mart-2021-goda.

[84] https://soliq.uz/activities/tax-risk-analysis?lang=ru

[85] https://soliq.uz/activities/debtor

[86] https://my.soliq.uz/nds/home?lang=ru&user_type=2

relationships between foreign structures (trusts) and residents, assessors find it difficult to conclude about the effectiveness of practical measures and base their evaluations only on theoretical judgments.

1129. In Uzbekistan there is an institution of fiduciary management, which differs from the trusts created in the countries with the Anglo-Saxon system of law, in which the identification of beneficiaries is as important as the BO. Fiduciary management in Uzbekistan does not refer to trusts or other legal arrangements, because it does not provide for the transfer of ownership rights. Competent authorities can always trace who owns the property in trust (see details in the analysis under Recommendation 25).

Timely access to adequate, accurate and current basic information and beneficial ownership information on legal persons and legal arrangements

1130. Competent authorities have unrestricted access to the adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner. The source of this information is SSRBE, data collected by the FIs and DNFBPs and those available on the website of other government agencies . They also have a wide range of tools to obtain such data using alternative methods (e.g. ORM, investigation), international cooperation (obtaining data, in some cases, takes about a month). The competent authorities mainly use data from the SSRBE and note its quality. At the same time, data from other sources are seen as having good quality and useful.

SSRBE

1131. Basic information on legal persons and BO data are collected in the SSRBE[87], which is managed by the PSA[88]. At minimum the public version of the Registry includes: TIN, information on the registering authority, date and number of registrations, name of the legal person, type, status (active, liquidated, in the process of liquidation), amount of the statutory fund, data on the founders (even if there are several) and their shares in the authorised capital, contacts (e-mail, telephone, address), and information on the head (name, TIN). The registry also contains BO information and data, access to which is restricted by law (passport number and series, place of residence of the applicant, copies of founding documents).

1132. Provision of data from SSRBE is fee-based, except for requests of state bodies and business entities. Until June 1, 2021, the LEAs and other state agencies received information on legal persons upon request from the PSA without any obstacles. From June 1, 2021, LEAs and a number of other state bodies obtained direct access to data from the systems of state registration and registration of business entities. Basic information about the legal person, including the composition of the founders and their share in the statutory fund of the organization, is also available in the Single State Register of Companies and Organizations (SSRCO) of the State Statistics Committee[89], on the trademark website[90], as well as the website of the Central Securities Depository[91] (information about the owners of the JSC shares). The State Register of NGOs is available on the website of the Ministry of Justice[92]. Information on these legal persons, including data on their founders and BO, is available to the competent authorities upon request.

Information collected by the FIs and DNFBPs

1133. When accepting legal persons for service, banks identify a natural person - the beneficiary by checking their identity; examining the ownership structure; the founders. The banks verify the

[87] https://fo.birdarcha.uz/pub/search
[88] https://davxizmat.uz/ru
[89] http://registr.stat.uz/enter_form/ru/index.php
[90] https://orginfo.uz/
[91] http://openinfo.uz/ru/
[92] https://www.minjust.uz/ru/interactive/reestr-nocommerce/

obtained data with the SSRBE[93], SSRCO[94] и on the trademark website[95]. Some banks use the World-Check database, international sources[96]. A number of banks have their own databases on the BO, which are formed by individual banks themselves on the basis of information on beneficial ownership that they have themselves, as well as from other sources of such information (open databases). Banks provide information on legal persons to the competent authorities without any obstacles.

1134. All DNFBPs collect basic information about their customers. However, not all DNFBPs understand how the BO should be determined and how such data is collected. Among all categories of DNFBPs represented in Uzbekistan, notaries, advocates and auditors identify BO and collect corresponding data. As a result of communication with the representatives of DNFBPs assessors concluded that they use the SSRBE as the main source of data, then the website of the State Statistics Committee[97] and other open sources. During the meetings, all DNFBPs noted that they provide information about their clients - legal persons at the request of the competent authorities without any obstacles. The FIU regularly interacts with the FIs and DNFBPs and is the main recipient of data. As a rule, information is provided by the FIU and DNFBPs in a fairly short period of time (from one hour to one day). LEAs request the FIU or contact FIs or DNFBP directly (in the framework of a criminal case) and receive all the necessary information. FIUs and LEAs reported that they had no difficulties in obtaining information from both the FIs and DNFBPs.

Access to basic information about legal persons and identification of BO

1135. The LEAs use additional sources when searching for information about the legal persons and the BO. Competent authorities cross-check data from public sources for reliability. Information is compared with the databases of state bodies, banks, ORM and investigative methods and FIU capabilities are used. The LEAs noted that there are no obstacles to searching, identifying and obtaining information about the legal person and the BO at the national level. Searching and obtaining such data takes less than a day in complex cases, and less than an hour in all other cases.

Case Study 5.5. (Identification of the BO of a legal person within the country)

FIU found that the branch manager of Gamma Bank, in order to steal credit resources, abusing her official powers, allocated a loan of 1.9 billion UZS for the purchase of household appliances for LLC "NRY", which belonged to her associate "A". Defendant "A" transferred the received credit funds to the account of LLC "AVD" for the purchase of household appliances. The funds were then sent to "NKA" LLC in the form of a financial loan. This LLC transferred them to the account of LLC "AOI" in the form of replenishment of the authorized capital, and later these funds were transferred to the account of LLC "MDO" again in the form of a financial loan. In the course of the investigation to identify the BO of the aforementioned legal persons, the FIU found that the manager of the Gamma bank branch was a shadow leader of the legal person "MDO", which ultimately received the allocated credit resources through a complex scheme of transferring them. It was also established that the manager of the bank branch sent a letter to Realtor LLC, according to which the real estate company held a closed auction for selling the bank's property (the store and the administrative building) at understated prices. In order to legalize loan funds, the manager of the Gamma bank branch purchased the bank's real estate at the auction. On February 3, 2020, the FIU initiated criminal proceedings against the manager of the Gamma bank branch and other defendants for embezzlement by misappropriation or extortion; abuse of power or official authority; and legalization of criminal proceeds. As a result of the investigation, the manager of the Gamma bank branch and other defendants were charged under the relevant articles of the CC. The criminal case was transferred to court.

[93] https://fo.birdarcha.uz/pub/search
[94] http://registr.stat.uz/enter_form/ru/index.php
[95] https://orginfo.uz/
[96] https://www.nalog.gov.ru/rn77/about_fts/inttax/oppintevasion/obdig/ (databases of foreign countries, the links are available on the website of the Federal Tax Service of Russia); https://egrul.nalog.ru/index.html (unified state register of legal persons on the website of the Federal Tax Service of Russia); https://opencorporates.com/ (the largest public database of companies in the world).
[97] http://registr.stat.uz/enter_form/ru/index.php

1136. LEAs, including FIU, noted that there may be difficulties in accessing the foreign accounts of legal persons and their BO. At the same time, it is noted that every request to FIUs of foreign countries related to a legal person is accompanied by a request to provide BO data. FIU also uses "World check online"; "Spark-Interfax"; international databases[98] and other sources. From 2016 to 2020, the FIU sent 366 international cooperation requests.

Case Study 5.6. (Identification of a legal person's BO abroad)

FIU conducted a parallel financial investigation at the request of the State Customs Committee of Uzbekistan on the facts of import contract at inflated prices. In analyzing foreign trade transactions, the SCC discovered imports of equipment by Cosmetics LLC worth USD 2.5 million. The price raised a reasonable suspicion of artificial overpricing. The SCC sent a request to the Turkish Ministry of Trade to clarify the export prices of the equipment. As a result, it turned out that the export value was artificially understated in relation to the import value by 30 (thirty) times. The materials received were submitted to the FIU for financial investigation and action. The FIU sent a request to the FIU of Turkey in order to establish the BO of the Turkish company "Ticaret Sirketi" and further cash flow. According to the information received, the BO of Ticaret Sirketi was a citizen of Uzbekistan. In the course of the investigation, the connection between Anvar and the founder of Cosmetics LLC was established. Based on the results of the preliminary investigation, the FIU initiated a criminal case for embezzlement and entering into a transaction contrary to the interests of Uzbekistan. The criminal case under the ML was not initiated.

Supervisory authorities

1137. Supervisors use the SSRBE, SSRCO, and other sources to collect data on legal persons and BO within the scope and purpose of their activities. For more information, see the analysis on achieving IO.3.

Access to and exchange of financial information

1138. Banks are required to notify the STC about the opening/closing of an account or deposit, changes in the details of the account or deposit of any legal or natural person in electronic form within 3 days. Taxpayers inform the STC about participation in the activities of legal persons registered both in Uzbekistan and abroad. At the time of the on-site mission, the STC had not received reports of participation in foreign legal persons or arrangements.

1139. The FIU and STC signed an Agreement on Cooperation dated 06.02.2019 No.4/8kk, according to which there is direct access to STC databases, including electronic invoices and data on bank accounts of taxpayers (STC has access to information on the accounts of legal persons in banks). Given the direct access of the FIU to the STC resources, there is no separate accounting for data exchange. The FIU may also have access to the materials of tax audits. In other cases, the STC may provide information at the request of the LEAs within one (1) day.

1140. In order to promote multilateral cooperation and implementation of OECD international standards, joining efforts to combat tax evasion or non-payment, as well as illegal financial flows, STC is working on Uzbekistan's accession to the OECD Global Forum on Transparency and Exchange of Tax Information. At the time of the on-site mission, according to STC representatives, six consultation meetings were held during 2020-2021.

Legal arrangements

1141. Information about residents who have a relationships or conduct financial transactions with a party to a foreign trust is collected by the FI and DNFBP when and during the establishment of the business relationship. This data is collected as part of the CDD. See also paras. 1117 and 1118. Legal

[98] https://find-and-update.company-information.service.gov.uk/; www.offshore-leaks.com; https://opencorporates.com/

arrangements are subject to the same provisions as legal persons with regard to ensuring timely access by competent authorities to adequate, accurate and current information.

Effectiveness, proportionality and dissuasiveness of sanctions

1142. The legislation provides for various sanctions for non-compliance with the requirements to provide information to competent authorities, including on legal persons. Sanctions are applied for failure to provide information on changes in the registration data of legal persons, as well as for failure to provide information at the request of LEAs on cases under their investigation. For non-compliance with the above requirements, individuals are sanctioned on the basis of the CAO (Art. 176 note 2, 194, 197, 198).

1143. Statistics on cases related to prosecution for failure to provide data on a legal person or its BO are not kept. During the interviews with the LEAs it was noted that there are no cases of non-submission of data by legal persons. Assessors tended to trust this information based on the context of the country and the measures taken by the competent authorities.

1144. There are no sanctions for providing inadequate, inaccurate, and not up to date information about a legal person during registration, which is a significant shortcoming. Nevertheless, assessors believe that pre and post-registration inspections by the competent authorities can identify mistakes in registration data and thus prevent inaccurate data from being provided. In Uzbekistan, officials are fined for failure to submit, late submission or submission of distorted data on the occurrence of taxpayers' liabilities. This is punishable by a fine of seven (7) to ten (10) RSV, and a fine of ten (10) to fifteen (15) RSV for committing this violation repeatedly within a year.

1145. The amount of sanctions, considering the average salary in the country, according to the competent authorities, is proportionate and dissuasive. Nevertheless, assessors do not agree with this opinion and believe that these sanctions may not have a dissuasive effect if applied to dishonest persons, given the amount of their income.

Table 5.6. Information on bringing to responsibility under Article 215 of the CAO (Violation of the procedure for presenting information on the emergence of taxpayers' obligations)

Indicators	Article 215-3 of the CoAO					Total
	2016	2017	2018	2019	2020	
Number of cases when administrative liability was imposed	149	79	111	394	110	843
Amount of imposed fines (UZS mln)	135,8	82,8	133,8	559,1	171,7	1083,3 or 101,7 thousand US dollars

* *Note*: based on the actual court orders.

1146. The CB did not impose sanctions on reporting entities for failure to identify the BO or to confirm the accuracy of data on legal persons due to the absence of such violations. Violation of the BO identification procedure is considered a serious violation by the CB. The list of measures and the amount of sanctions are determined by the CB on the basis of data obtained from the results of supervision.

1147. The sanctions for non-compliance with information requirements applied to legal and natural persons are assessed as requiring significant strengthening to the extent that this would be sufficient for their greater effectiveness, proportionality and dissuasive effect.

Overall conclusion on IO.5

1148. Information on the creation and categories of legal persons in the country is publicly available. The SSRBE contains basic information on legal persons and BO. The registry is maintained by the PSA, and the registration of legal persons is carried out by the PSC. Legal arrangements, in the sense in which this term is used in the FATF Recommendations, cannot be created in Uzbekistan.

1149. Competent authorities have demonstrated a good understanding of how legal persons are used for illicit purposes. An assessment of their inherent vulnerabilities was made during the NRA. According to the results of the NRA, LLCs are the most common type of legal persons used for illegal purposes. The LEAs identify typical cases of legal persons being used for illicit purposes. Competent authorities are not sufficiently aware of the vulnerabilities that can come from the misuse of professional accountants and legal practitioners.

1150. The Republic of Uzbekistan has created conditions to mitigate the illicit use of legal persons. The measures taken include ensuring the accuracy and up-to-date information in the SSRBE; inspections of legal persons; LEAs measures; improvement of legislative acts; interaction of competent authorities among themselves and with reporting entities; maintenance of the SSRBE and keeping its data up to date, predominance of non-cash settlements, denials in state registration and acceptance for service in banks.

1151. The SSRBE is publicly available and is considered as the main source of basic information on legal persons and BO. Competent authorities have unconditional access to the SSRBE, to the data of the FIs and DNFBPs, as well as considerable possibilities for obtaining information on legal persons and BO using other methods. There are no obstacles for the competent authorities to search, identify and obtain basic information about legal persons and BO at the national level. At the same time, there may be difficulties with access to information on accounts of legal persons opened abroad, and their BO.

1152. Fines do not apply to persons for providing inaccurate or unreliable information during registration. Fines for failure to comply with requirements to store and provide basic information about the legal person and BO, as well as limited measures against some DNFBPs for failure to collect the said information are considered by assessors as not sufficient, they can be strengthened. There is a liability against officials for failure to provide data on the occurrence of taxpayers' liabilities.

1153. **The Republic of Uzbekistan is rated as having a moderate level of effectiveness for IO.5.**

CHAPTER 8. INTERNATIONAL COOPERATION

Key Findings and Recommended Actions

Key Findings

1. The republic provides legal assistance in a constructive and timely manner, fulfilling 800-900 requests for legal assistance annually. Being the coordinator of this activity, GPO ensures the fulfillment of most requests within up to 3 months. Secure electronic communication channels, along with other means, are used for the transmission of requests. The FATF Global Network survey gives a positive estimate of the quality of MLA delivery.
2. In most cases, all competent authorities employ MLA mechanisms, if the case involves a transnational element. Statistics indicate that the competent authorities confidently use MLA, even when it concerns non-CIS countries (North America, Europe). In general, the requested assistance corresponds to the risk profile of the country; however, the amount of MLA requested in "transit" jurisdictions, in particular, in the Republic of Uzbekistan, is insignificant.
3. LEAs use the MLA mechanism to search for assets, but priority is given to other forms of cooperation. Seizure of property abroad results in sending a confiscation request.
4. The state authorities effectively cooperate in the extradition of criminals. The number of incoming extradition requests is small and most of them are approved. There are no cases of refusal to extradite accused of ML/TF. Cases from foreign countries are properly investigated and prosecuted.
5. In cases where a person has escaped from LEAs, the authorities of the state take measures to establish his whereabouts and subsequently seek his extradition. In just 5 years, extradition was requested more than 2 thousand times and it was granted in the overwhelming majority of cases. Few cases of postponement of extradition in connection with the serving of sentences were potentially associated with FT offences.
6. There is a practice of transferring criminal cases to a foreign state for criminal prosecution. However, their number is half the number of cases of refusal to extradite and is not connected with cases of terrorism. GPO receives and requests information on the outcome of such cases, but such information is not generalized on a systematic basis.
7. Information exchange through the FIU is carried out perpetually, together with a wide range of partners, and its nature corresponds to the national ML/TF risks. Representatives of the FIU demonstrated various instruments and channels of international interaction that can cover not only the needs of financial intelligence itself but also of other LEAs. However, more attention needs to be paid to this communication channel. Statistics of incoming and outgoing requests and spontaneous messages demonstrate Uzbekistan's moderate approach of Uzbekistan to information search through the FIU channels.
8. International collaboration on issues of supervision is limited. Supervisory bodies for financial institutions are parties to international agreements and participate in other relevant international organizations; there are no legislative impediments to the information exchange. However, the actual interaction in the AML/CFT line is carried out only by the Central Bank. Due to their specifics, other supervisory authorities did not need to exchange such information.
9. All competent authorities are able to receive and transmit information on BO through MLA channels, but there is no common understanding of the plan of action to collect appropriate data in such cases. In many ways, the value of information depends on the attention paid to a specific request. Also, law enforcement agencies have not yet sent requests for information on BO through MLA mechanisms.

Recommended Actions

1. Competent authorities should keep expanding the use of MLA mechanisms and other forms of cooperation to trace, seize and confiscate ML/TF proceeds. If there are preventing gaps in laws and other legal acts, then legislative amendments should be made. Training in this area should be

intensified to enable competent authorities to prepare high-quality requests for the return of proceeds laundered abroad.

2. The Republic of Uzbekistan should establish mechanisms of the quality control of the provided legal assistance. It should request feedback systematically, accumulate data about the usefulness of the transmitted information, analyzing it and taking measures to improve the quality of MLA.
3. Competent authorities should intensify the use of international cooperation requests where there is a link between criminal activity and offshore jurisdictions and 'transit' countries, as well as srengthening customs cooperation in order to detect illegal imports of currency, including for the purpose of subsequent ML/TF within the country.
4. In view of the fact that, in accordance with the NRA, as a rule, TF activities were carried out by convicted citizens of Uzbekistan outside the country, the Republic of Uzbekistan needs to pay more attention to spontaneous reporting when these facts are revealed.
5. The country's authorities need to continue developing the existing mechanisms to control postponed extradition when a person is serving a sentence in a foreign country and to request their temporary extradition more often.
6. Central authorities should continue systematical recording of detailed statistics on MLA granted and received, extradition, and transfer of prosecutions to foreign states, in particular, in the context of ML/TF and predicate offenses.
7. LEAs need to develop a unified methodology for identifying BO when fulfilling MLA requests as well; and also they need to provide appropriate training for employees, which should include practical methods of identifying BO in foreign jurisdictions.

Immediate Outcome 2 (International Cooperation)

1154. In this section the achievement of Immediate Outcome 2 is examined and assessed. In assessing effectiveness in this part, Recommendations 36-40 are used.

Providing constructive and timely MLA and extradition

1155. The Republic of Uzbekistan has created a proper legal framework for the rendering of MLA and extradition. At the same time, the country's authorities make efforts to improve and finalize legal mechanisms. In general, the competent authorities strive to provide constructive and timely legal assistance and to carry out extradition promptly.

Mutual legal assistance

1156. As part of the survey of members of the FATF Global Network, the Republic of Uzbekistan received predominantly positive or neutral feedback on the quality and timing of MLA.[99] At the same time, the statistics and examples provided by the Republic of Uzbekistan convincingly testify that providing MLA is positive in most cases, despite the geographical remoteness of jurisdictions and other related factors.

1157. There are several central bodies in the country (SC, MIA, SSS, GPO), which can act directly in accordance with international treaties of the Republic of Uzbekistan or on the basis of the principle of reciprocity. At the stage of judicial consideration of the case, MLA is carried out through the Supreme Court, and in the course of pre-trial proceedings, it is carried through other bodies within their competence according to the criminal procedure legislation.

1158. Since May 2021, GPO has been the coordinator of MLA. Even previously, however, it was the actual coordinator of this activity, being the central authority for a number of international treaties and also in cases where the fulfillment of the request had been associated with a court decision. The requests

[99] In total, 12 countries, including the Russian Federation, Turkmenistan, the Republic of Kazakhstan, the Republic of Kyrgyzstan, the Republic of Belarus, the Republic of Tajikistan, Turkey, Denmark, Canada, Jordan, and Germany, sent feedback on responses.

received by GPO are forwarded to be fulfilled to the competent authorities. MIA and SSS can fulfill requests received directly within the framework of the Minsk and Chisinau conventions. In the Republic of Uzbekistan, there are flexible rules for transferring MLA requests between central authorities, which allow, even in cases where the request was received by the authority by mistake, to send it in accordance with the competence without returning or refusing to fulfill it.

1159. Upon receipt of MLA requests, they are reviewed for compliance with international treaty requirements as well as with domestic legislation. It should be noted that the presence of dual criminality, as well as the literal correspondence of the names of the norms of the criminal law, are not grounds for refusing to grant MLA in cases where such assistance is not associated with coercive measures. In fact, all incoming MLA requests are fulfilled, and substantive answers are given to them. Once the request has been checked, it is handed over to the executing officer (investigator, inquirer).

1160. For the transmission and distribution of requests, the usual rules of office correspondence are applied, as well as additional requirements established by the interagency directive, which guarantee the confidentiality of information and promptness of its transfer. The office management system is based on electronic document management (EDM), which allows significantly reduces the time for transferring information and ensure meeting deadlines for responses, which results in the promptness of the interaction.

1161. The administration of MLA requests is carried out at the specialized subdivisions of the central offices of the competent authorities; as well as at their territorial bodies, by authorized officers. At the same time, the authorities of the country pay serious attention to the issues of training and professional improvement of officers involved in international cooperation. So, over the past 5 years, 278 officers have undergone advanced professional training in the Academy of the General Prosecutor's Office, and among them 8 officers studied in the field of international cooperation in the area of AML/CFT.

1162. Despite the relatively small number of human resources (the GPO has 4 people, and the MIA has 2, according to information on the agencies' central offices), the effective organization of the MLA system allows the competent authorities to provide a significant amount of legal assistance within a short time - up to 1 month. For example, each year, the MIA, acting as the central authority, executes around 700 requests. Besides, about 100 requests the said body receives through the GPO.

Table 2.1. The number of received and fulfilled requests through the GPO

		2016	2017	2018	2019	2020	Total
Received		354	396	415	262	160	1 587
of which transferred to	the General Prosecutor's Office	174	228	161	75	43	681
	the MIA	134	89	87	126	87	532
	the SSS	46	79	167	61	30	383
Fulfilled		350	390	411	259	159	1 569
of which	by the General Prosecutor's Office	173	224	161	75	43	676
	by the MIA	132	88	87	123	86	516
	by the SSS	45	78	163	61	30	377

Table 2.2. The number of received and fulfilled requests by the MIA directly

	2016	2017	2018	2019	2020	Total
Received	690	581	659	668	558	3156
Fulfilled	The number of fulfilled requests fully corresponds to the number of requests received					

Table 2.3. The number of received and fulfilled requests by the SSS directly

		2016	2017	2018	2019	2020	Total
Received	ML	No MLA requests on ML were sent to the SSS directly					
	TF	0	0	12	13	1	26
Fulfilled		The number of fulfilled requests fully corresponds to the number of received requests					

1163. The Republic of Uzbekistan is flexible and effective in choosing the procedures for granting and accepting MLA. When necessary, Uzbekistan contacts directly with cross-border partners, including Kazakhstan (2004 agreement), Kyrgyzstan (2006 agreement), and Tajikistan (2018 agreement). This allows the prosecution authorities to bypass the central office and to receive the necessary information directly through the MLA mechanisms from the competent authorities of foreign states in the adjacent areas. According to the opinion of assessors, the amount of communications through these channels is not large (27 incoming requests and 18 outgoing requests in 5 years for all countries). Nevertheless, the very fact of these communications helps to believe that the authorities strive to provide MLA effectively.

1164. All incoming MLA requests are processed fairly quickly. By default, according to the interagency directive, the deadline for the fulfillment of an incoming request is 30 days. As a rule, the period of fulfillment does not exceed 3 months if requests are received through the General Prosecutor's Office. But in most cases, this period is shorter and is no more than a month by default, and in simple cases, it is up to 14 days. Less than a quarter of incoming requests are fulfilled in a period of more than 3 months. It should be noted that even complex ML/FT-related requests are generally performed within 3 months. For example, 89 ML-related requests were performed for the last 2 years, 63 (70&) of them were performed within 3 months, and the rest were performed within 6 months. Longer periods are sporadic and they take place due to the complexity of cases, a large amount of data collected, and the necessity to obtain additional information about the request from its initiator. If requests are submitted directly to the MIA, they are fulfilled in the same term or sooner. This promptness in the fulfillment of requests is convincing proof of the functioning of the MLA system.

Table 2.4. Terms of the fulfillment of requests received through GPO[100]

Fulfilled	2016	2017	2018	2019	2020	Total
up to 3 months	328	375	401	252	81	91,6%
up to 6 months	22	15	10	7	78	8,4%

1165. Representatives of the competent authorities indicated the high-quality fulfillment of requests to be their priority. However, criteria of high quality are based on their own practice only and do not correspond to the actual usage of provided responses in foreign jurisdictions. All central authorities reported at meetings that they claim feedback never or rarely. Instead, due to close contacts with representatives of foreign competent authorities, information on the usage of the responses can be obtained on a routine basis. But the absence of the relevant databases indicates the fact that accumulation and analysis of such information, if any, are not of a systematic nature.

1166. The Republic of Uzbekistan provided expanded statistics on MLA provision in the context of ML, TF and predicate offenses for the last 2 years and also general numbers on received and fulfilled requests for 5 years. At the same time, the GPO, being the coordinator of this field, began to accumulate general data on MLA requests received by all central bodies as recently as 2021. While the statistics provided generally allowed for an assessment of the country's efforts to provide the MLA as significant, the nature of the data provided suggests that statistical data had not previously been collected regularly. Thus, in addition to the above limitation of 2 years for general data, the MIA was only able to provide the total number of enquiries received bypassing the GPO and the number of fulfilled requests. The timing of the submission of this data to the assessors is evidence that the country has only recently created a unified approach to the formation of statistics in the area in question.

1167. According to information provided by GPO, there were no MLA requests for tracing, seizure and recovery of assets. At the same time, the legislation of the republic allows for the implementation of such procedures; and the competent authorities have shown perfect understanding of this issue and

[100] The statistics in this table include requests sent for fulfillment by the General Prosecutor's Office to the Ministry of Internal Affairs and the State Security Service.

gave examples when the information transferred by a foreign jurisdiction was connected with the disclosure of banking secrets.

Case study 2.1. (Example of bank secret information provided within MLA)
GPO at the beginning of 2021 fulfilled the request of the competent authorities of the MIA of the Republic of Lithuania concerning a criminal case on the legalization of property, which was obtained by crime. For legalization, a legal entity, a resident of the Republic of Lithuania through economic entities in the Republic of Uzbekistan concluded fictitious transactions of sale and purchase of information technology and visualization equipment. The fulfillment of the request implied obtaining an account statement from one of the banks of the Republic of Uzbekistan, as well as documents concerning the usage of client bank software, including IP addresses and information about persons who digitally signed payment documents. The investigator of the prosecutor's office, having received the prosecutor's sanction, seized all the listed documents in the bank. Thereafter they were sent to the initiator of the request.

1168. The above example shows that even when there were certain restrictions in the legislation (for details see Clause) regarding the receipt by the competent authorities of information constituting bank secrecy, law enforcement practice was sufficiently flexible[101] in addressing the issue of meeting the relevant needs for information of law enforcement agencies, including MLA. However, due to the small law enforcement experience in relevant cases, the executive officer may lack understanding of the plan of activity required in the field of tracing and seizing assets. Notably, by the end of the on-site mission, amendments to the Bank Secrecy Law were approved, which will facilitate the information exchange between the competent authorities, while observing the necessary confidentiality requirements.

Extradition

1169. In the assessed country requests are considered through administrative procedures, and the decisions made are appealed through the courts. GPO is empowered to consider extradition requests; and relevant decisions are made by the Prosecutor General or his deputies. Besides, the legislation provides for strict deadlines for considering incoming requests, and in the general case, this term is 20 days.

1170. The Republic of Uzbekistan annually receives an average of 10 extradition requests; in total, 51 requests were received from 2016 to 2020. Most of them are satisfied (41), but in some cases, they are refused (10). The refusal in 3 cases was due to the expiration of the statute of limitations for a criminal prosecution; and 7 refusals were sent because either criminal prosecution was instituted already in the Republic of Uzbekistan or the legislation had not provided for imprisonment for the crime in question. Among the requests for extradition in 5 years, only one concerned ML (see example 2.1), and there were no requests related to TF.

Case study 2.2. (Extradition to a foreign country in a criminal ML case)
The competent authorities of the Republic of Kazakhstan investigated a criminal case of embezzlement of funds and the legalization of criminal proceeds in the amount of $7.5 billion. The person involved in the crime was detained in the Republic of Uzbekistan. In this connection, the General Prosecutor's Office of the Republic of Kazakhstan in December 2018 sent a request for his extradition to the General Prosecutor's Office of the Republic of Uzbekistan.
As the request underwent consideration, a decision was made in January 2019 to extradite the detained person to the law enforcement agencies of the Republic of Kazakhstan.

1171. As a rule, extradition is carried out under international treaties and bilateral agreements, or under the principle of reciprocity, in case the said treaties and agreements are absent. In the past 5 years, 10 persons have been extradited to one of the jurisdictions on the basis of reciprocity.

1172. In practical terms, all extradition measures, including the provisions concerning convoy and transportation of the extradited person, are carried out by the MIA after confirmation from the GPO.

[101] For the purpose of the relevant goals, law enforcement agencies and courts used extensive interpretation of the Bank Secrecy Law.

1173. The legislation of the Republic of Uzbekistan does not prohibit extradition under simplified procedures. That said, a number of bilateral international treaties which can be enforced directly, provide for the extradition without the relevant procedures, subject to the consent of the involved person. For example, article 12 of the Agreement between the Republic of Uzbekistan and the Republic of Turkey on extradition (Tashkent, 20.04.2018). The Republic of Uzbekistan also provides assistance in search and detention. In such cases, requests are considered by the MIA under existing bilateral agreements.

Case study 2.3. (Example of assistance in extradition)
MIA of the Republic of Tajikistan sent a request via closed communication channels for assistance in the arrest of the wanted citizen of the Republic of Tajikistan, A, who was staying in Tashkent. The field officers of the MIA and the SSS of the Republic of Uzbekistan detained the wanted person in course of joint operations. After the arrest, the person was transferred to the officers of MIA of the Republic of Tajikistan for further investigation.

1174. The Republic of Uzbekistan, according to the current Constitution, does not extradite its citizens. However, there have been no refusals to extradite under such a basis in the past 5 years. Besides, national legislation provides for the possibility to bring to criminal responsibility on the territory of the country, under the request received from foreign authorities. In total, 83 criminal cases (all related to the predicate offences) for further criminal prosecution have been received in the Republic of Uzbekistan in 5 years. Most of such cases come from the CIS states, while cases from non-CIS states are few (just 3 in the same period).

Case study 2.4. (An example of criminal prosecution in the Republic of Uzbekistan at the request of a foreign state)
The competent authorities of the Russian Federation investigated a criminal case involving bribery committed by a citizen of the Republic of Uzbekistan on the territory of the Russian Federation. Because the person accused of committing this crime was hiding in the Republic of Uzbekistan, the Prosecutor General's Office of the Russian Federation sent a request to the GPO of the Republic of Uzbekistan in late 2018 to carry out criminal prosecution against him.
A preliminary investigation was carried out in the Republic of Uzbekistan based on the request, and the criminal case was sent to court. In April 2019, the Uzbek national was found guilty of bribery.

1175. The legislation of the Republic of Uzbekistan stipulates mandatory requirements to send information about the final procedural decisions on such cases to the GPO, which in each case provides feedback to the country initiating the request. The demonstrated practical work shows the open cooperation of the Republic of Uzbekistan on the issue of extradition at the international level.

1176. The competent and central authorities of the Republic of Uzbekistan, substantially, provide MLA and settle issues of extradition in a timely and constructive manner. Moderate improvements are needed.

Seeking timely legal assistance to pursue domestic ML, associated predicates and TF cases with transnational elements

1177. The NRA results, as well as additional information provided by the country, indicate that a considerable proportion of predicate offenses and ML/TF cases is of cross-border nature. In particular, the above said is testified by considerable money transfers abroad and from abroad, sizeable cash flows to offshore jurisdictions, and participation of terrorists who are citizens of the Republic of Uzbekistan in both local and international terrorist organizations.

1178. Competent authorities are well aware of the risks involved and strive to properly investigate the transnational aspect of crime, where possible, also by resorting to MLA mechanisms, requesting extradition, and issuing orders to carry out criminal prosecutions.

Mutual legal assistance

1179. The competent authorities of the Republic of Uzbekistan initiate 300-400 MLA requests on average. Most of these requests are sent through GPO, and a minor part is sent directly by the MIA as the central authority. The SSS is also able to send requests directly.

Table 2.5. The number of requests sent through GPO and of responses received

		2016	2017	2018	2019	2020	Total
Sent		242	259	260	153	63	977
of which transferred to	GPO	79	90	56	46	19	290
	MIA	135	147	123	74	33	512
	SSS	28	22	81	33	11	175
Responses received		223	242	247	147	59	918
of which on request	GPO	78	87	53	46	19	283
	MIA	118	135	114	70	29	466
	SSS	27	20	80	31	11	169

Table 2.6. Number of requests sent directly by the MIA and responses to them

	2016	2017	2018	2019	2020	Total
Requests sent	248	161	170	128	83	790
Responses received	193	117	122	96	35	563 (71,3%)[102]

Table 2.7. Number of requests sent directly by the SSS and responses to them

		2016	2017	2018	2019	2020	Total
Requests sent	ML	2	2	1	0	0	5
	TF	1	3	0	1	1	6
	Predicate offences	2	4	1	1	2	10
Responses received		The number of fulfilled MLA requests fully coincides with the number of sent requests					

1180. The amount of the requested MLA seems to be considerable, but just a portion of requests concerns transnational crimes, as well as predicate crimes, terrorist crimes, and cases of ML/TF. Some TF inquiries were sent directly by the SSS. Also, some MLA requests concerning ML cases were also sent by the aforementioned body.

Table 2.8. Number of MLA requests concerning transnational crimes and their share in the total number of MLA requests sent[103]

	2016	2017	2018	2019	2020	Total
Number of MLA requests on crimes with a transnational component	86	117	109	51	33	396
The share of MLA requests on crimes with a transnational component in the total number of requests sent	35,5%	45,2%	41,9%	33,3%	52,4%	40,5%

Table 2.9. Number of MLA requests sent and fulfilled related to the investigation of predicate offenses with features of ML and terrorism[104]

	2019	2020	Total
Number of requests on predicate offenses related to ML	72	36	108
Number of ML criminal cases initiated in the relevant period	39	48	87
Number of requests on terrorist crimes	7	9	16
Number of criminal cases on terrorist offenses initiated in the relevant period	103	96	199

1181. The above data on the number of MLA requests on criminal cases with ML features, in comparison with the number of initiated ML cases, testify to the fact that the state's competent authorities thoroughly investigate schemes of criminal proceeds and strive to search for the transnational element

[102] Proportion to the number of requests sent directly by the MIA
[103] Statistics are provided on requests sent through the GPO
[104] Statistics are provided on requests sent through the GPO

without waiting for the formal evidence sufficient to initiate an ML case, using national resources of information. The competent authorities of the Republic of Uzbekistan in the CFT issues prefer to use informal cooperation and other forms of data exchange in addition to MLA. The effectiveness of this approach is confirmed by the results of work on countering terrorism and TF (see below for more details). Thus, despite the absence of MLA requests focused exclusively on ML and TF, the state's authorities nearly always resort to MLA procedures when it comes to searching for the transnational element in ML and TF schemes.

1182. It should be noted that the statistics on MLA requests sent through GPO in 2016-2018 present only the quantity of orders sent and fulfilled by the competent authorities of foreign states. There is no extensive data on the requests. A similar situation takes place on requests sent directly by the MIA and the SSS. This once again testifies to the conclusion that the Republic of Uzbekistan has just recently begun to take an interest in the effectiveness of the requested legal assistance; so the extensive measures taken by the country's authorities to improve work in this field are still awaiting their result.

1183. LEAs in the Republic of Uzbekistan use MLA mechanisms to trace assets abroad. According to data for the last 5 years, 19 such requests were sent, in particular, to Spain, France, the Czech Republic, Latvia, Russia, and Kazakhstan. At the same time, according to the explanations of the competent authorities, in asset tracing priority is given to other forms of cooperation, including FIU channels and others. Virtually in all cases where MLA asset tracing mechanisms have been used, the subsequent action has resulted in the seizure and recovery of the detected property. In the period from 2016 to 2020, 17 requests in total were sent for seizure and subsequent return of property to the Republic of Uzbekistan (all related to ML).

Case study 2.5. (Example of arrest on ML case due to MLA)
In an investigated criminal case against members of an organized criminal group (OCG) of N and others, in 2014 requests for MLA were sent to the competent authorities of the Russian Federation to identify real estate objects acquired with the criminal proceeds by members of the OCG on the territory of the Russian Federation. As a result of close interaction in 2015-2018, 15 real estate objects, several bank accounts, and safe deposit boxes with jewelry were identified. Of the assets identified in Russia, there were 6 high-value real estate objects, incl. 1 hotel complex, and 2 bank accounts issued with persons not associated with the committed crimes (a housemaid and a driver) who voluntarily declared these assets. In 2020, due to the request of the Republic of Uzbekistan for the acknowledgment and enforcement of sentences regarding confiscation, some of the real estate objects and bank accounts arrested in Russia were confiscated under the decision of the Russian court.

1184. The absence of the requests for tracing of TF assets, and of seizures of TF assets abroad indicates the necessity for the state's authorities to make additional efforts for tracing terrorists' assets abroad. This aspect is also crucial, since, according to repeated statements of the competent authorities of the Republic of Uzbekistan, most cases of terrorist financing are committed by citizens of the country outside of borders, which means FTF assets to be located inevitably abroad.

1185. Competent authorities stated that they are by no means limited in providing feedback on responses to MLA requests directed by them. Nevertheless, they do not initiate such feedback on their own, and there are no statistics on this issue.

1186. The number of requests sent to each country corresponds in general to the amount of cash outflows country-wise. However, the risks associated with some jurisdictions correspond just to a certain degree with the frequency of information requests. Thus, the amount of MLA requests for some jurisdictions appears to be too small. For example, the Republic of Cyprus, which is in the top position in terms of the amount of cash outflows from the Republic of Uzbekistan, was the addressee of requests only in three cases in 5 years. The leading trade partner of the Republic of Uzbekistan, the PRC, also just in a few cases became an object for receiving MLA.

1187. When requests are sent through the GPO, they are implemented by its officials, who contact the executive officer on a routine basis, and also, if necessary, remind them in writing about the waiting

for a response. The initiators of requests are also authorized to establish direct contacts with the executive officers, and they strive to resort to such procedures in cases where the request implies eventful and complex investigative actions. The officers of the competent authorities are sent to foreign countries to directly participate in investigative actions, if it is required by the nature of the criminal case.

1188. The statistics provided by GPO[105] show that in most cases the country fulfills requests with reasonable dispatch. That said, since the issue of the instructive regulation, the principles of prioritizing complicated requests have been used on a systematic basis. As the authorities report, before the issue of the regulation the dispatch of the requests was ensured by the marks “urgent” and “very urgent”.

1189. Information and telecommunication technologies, being implemented in the document control system of the Republic of Uzbekistan assuredly accelerate the forwarding of requests within the country. Moreover, even in cooperation with foreign colleagues, the country's authorities follow the same trend, using secure information transmission lines along with liaison officers and diplomatic channels to transmit MLA requests.

Case study 2.6. (Use of the VPN channel by the GPO)
In 2019, GPO, together with foreign partners, created a special secure VPN channel for exchanging MLA requests. Through the channel, requests and responses can be transmitted and received. The connection to the channel is carried out through a special key, with protection against phishing and network attacks. Extradition materials are also transmitted through the channel. So, for the period from 2019 to 2020, more than 500 requests were transmitted and considered through the channel.

1190. The competent authorities of the Republic of Uzbekistan have demonstrated a thorough understanding of MLA potential and of methods of implementation of relevant mechanisms in the investigation. Besides, in complicated cases, investigators and operational officers are sent to foreign countries for direct participation in investigative actions. Thus, in the period from 2016 to 2020, 18 officers of the operational and investigative units of the MIA were sent to foreign states (Russia, Kazakhstan, Kyrgyzstan) to carry out the necessary operational and investigative actions (not including detention) in 8 criminal cases.

Table 2.10. The number of investigative actions carried out by investigators of the GPO abroad and the number of investigators who took part in them

	2016	2017	2018	2019	2020	Total
Number of investigative actions	4	5	2	2	1	14
Number of investigators	8	14	6	6	5	39

Extradition

1191. The Republic of Uzbekistan actively requests extradition in cases where the investigation falls within its competence. Thus, over the past 5 years, more than 2 thousand requests were sent, most of which were satisfied. Only 27 extradition requests were related to money laundering and one of them was related to the financing of terrorism.

Table 2.11. Number of extradition requests sent by the Republic of Uzbekistan, relevant responses and their grounds

			2016	2017	2018	2019	2020	Total
Extradition requests sent			485	617	512	455	191	2260
Responses received[106]	satisfied		460	577	459	393	173	2062
	refused		19	23	26	38	11	122
	including	foreign citizenship	2	3	1	3	0	9
		expiration of the statute of limitations	6	1	5	14	7	33
		non-compliance with the	8	13	13	14	2	50

[105] Also it includes requests sent by the SSS and the MIA through the General Prosecutor's Office.
[106] The number of examined requests fully corresponds to the number of extradition requests sent

		principle of double criminality						
		asylum application	1	0	2	1	0	4
		Other grounds	2	6	5	6	2	20
	Postponement due to serving a sentence		6	17	27	24	7	81

Case study 2.7. (Extradition to the Republic of Uzbekistan in a criminal case on money laundering)
A criminal case on fraud, pseudo-business, forgery of documents, incitement to bribe, official forgery, and legalization of criminal proceeds was in the proceedings of the competent authorities of the Republic of Uzbekistan. The accused of these crimes was found on the territory of the Republic of Kazakhstan. In this connection, in June 2017 GPO of the Republic of Uzbekistan sent a request to the competent authorities of the Republic of Kazakhstan for the extradition of the wanted person. Subsequently, the detained person was transferred by the competent authorities of the Republic of Kazakhstan to the law enforcement agencies of the Republic of Uzbekistan.
In September 2017, the transferred person was found guilty by the court of the Republic of Uzbekistan and sentenced to 7 years in prison.

Case study 2.8. (Extradition to the Republic of Uzbekistan in a criminal case on the financing of terrorism)
In the proceedings of the competent authorities of the Republic of Uzbekistan, there was a criminal case initiated on the facts of financing terrorism, encroachment on the constitutional system of the Republic of Uzbekistan, production, storage, distribution, or demonstration of materials containing a threat to public safety, participation in prohibited organizations. It was established that the person associated with these crimes financed international terrorist organizations by channeling criminal proceeds to the purchase of firearms, ammunition, explosives, food, and other items. The accused of committing the above-listed crimes has been found on the territory of Ukraine.
In this regard, in 2017 GPO of the Republic of Uzbekistan sent a request to the competent authorities of Ukraine for the extradition of the wanted person.
According to the results of the extradition check, in 2020 the detained person was transferred to the law enforcement agencies of the Republic of Uzbekistan.

1192. The average time for fulfilling extradition requests is 5 to 7 months, which seems to be quite fast in terms of the statute of limitations for criminal liability for money laundering and terrorist financing. A small number of refused and postponed extraditions of the requested persons corresponds to criminal cases potentially related to TF. The country's authorities explained that the majority of such cases were related to serving a sentence by a person in a foreign state. Such data indicate the need for effective control over the expiration of sentences and the extended practice of temporary extradition, which is limited.

1193. Notably, the statistics on cases of extradition requested and granted were revised by the Republic of Uzbekistan in the course of the on-site mission. Taking into account the nature of the corrected information, it demonstrates the lack of a systematic approach to recording and collecting such data.

1194. The Republic of Uzbekistan has the capacity and is striving to take all comprehensive measures to bring a person to criminal responsibility, even in cases of refusal to extradite the accused; which measures include, among others, sending the materials of the criminal case to a foreign state for criminal prosecution. However, such criminal cases make up no more than a quarter of the number of refusals to extradite and are not related to terrorism crimes[107], which account for most of the refusals. The major part of such cases is sent to the CIS countries.

[107] Categories of crimes for which criminal cases were transferred to foreign states: against the person - 7 cases, against health - 3, against traffic safety and operation of transport - 1, against freedom, honor and dignity - 3, theft of other people's property - 6, against the fundamentals of the economy - 5, against the order of functioning of authorities, administration and public organizations - 7, against public safety - 7, illegal circulation of narcotic drugs or psychotropic substances - 8.

Table 2.12. Number of criminal cases sent to foreign states for criminal prosecution

	2016	2017	2018	2019	2020	Total
Cases sent	5	13	20	8	1	47
including to the CIS countries	5	10	20	6	0	41

1195. The GPO mandatorily asks to be notified of the results of consideration of criminal cases sent for criminal prosecution to a foreign state. Relevant information is summarized systematically in the international cooperation department of the said agency.

Seeking other forms of international cooperation for AML/CFT purposes

FIU

1196. The DCEC has established contacts with the FIU of more than 160 foreign countries via the secure channel of the Egmont Group (Egmont's Secure Web system). The DCEC has been a member of the Egmont Group since 2011 and cooperates with foreign FIUs, both members, and non-members of the Egmont Group. The DCEC initiated and signed 22 Agreements and Memorandums of cooperation, in order to establish a legal framework and expand interagency cooperation with the competent authorities of foreign countries. In particular, 17 Agreements and Memorandums of Cooperation were signed with the FIUs of Bangladesh, Belarus, Kazakhstan, Cyprus, China, Korea, Kyrgyzstan, India, Indonesia, Israel, Poland, Russia, Ukraine, Japan, Afghanistan, Turkmenistan, and Turkey. Also, the DCEC signed agreements and a Memorandum with the competent authorities of Kyrgyzstan (the State Service for Combatting Economic Crimes), the United States (DEA and SS of DHS), Belarus (Financial Investigations Department), Tajikistan (Anti-Corruption Agency) in the field of combating tax and financial crimes. Most of these countries are either neighbours of Uzbekistan or have significant trade or migration flows or significant outward cash flows (Cyprus, China, etc.).

1197. In accordance with the Decree of the President of the Republic of Uzbekistan "On joining an international agreement" No. PP-3615 dated 19 March 2018, the Republic of Uzbekistan has joined the CIS Council of the Heads of Financial Intelligence Units (CH FIU CIS). Within the frames of CH FIU CIS, the DCEC participates in “Milky Way” and “Barrier” operations, aimed at enhancement of the combat against money laundering and financing of terrorism.

1198. In particular, the DCEC, within the “Milky Way” project, carried out verification and established monitoring of more than 860 entities included in the list of foreign technical companies, organizations acting as their nominal partners, as well as banks exposed to a high risk of being used for money laundering. These companies are constantly in monitoring and each operation carried out by these companies is checked for signs of money laundering. During the verification, 5 companies were identified as founders or co-founders of joint (foreign) enterprises in the Republic of Uzbekistan; also, 2 companies underwent verification due to STR.

1199. If, on the grounds of the results of financial monitoring, entities of foreign countries or operations related to foreign countries fall under suspicion of money laundering, predicate offenses or terrorist financing, the DCEC draws up and sends a request to the FIU of the respective country.

1200. A request is drawn up and sent as a matter of priority if it concerns the financing of terrorism or crimes of very high and high risk according to the national assessment of the risks of money laundering and terrorism financing.

1201. When conducting financial investigations with a foreign component, the DCEC systematically requests information from foreign FIUs. The intensity of requests varies, but in general, remains at the same level. The number of the sent requests, both ML and TF-related, exceeds the number of the received requests, which indicates a greater focus of the Republic of Uzbekistan on international cooperation and correlates with the risks identified based on the NRA.

Table 2.13. Number of international requests sent and received by the FIU

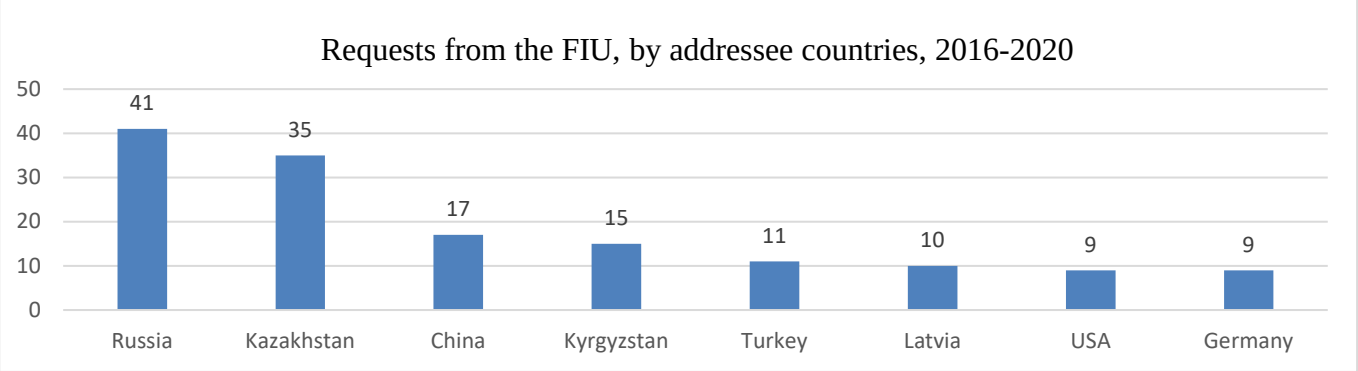
Год	Requests Sent	Requests Received

	ML	TF	ML	TF
2016	29	5	22	26
2017	180	15	24	27
2018	31	57	26	15
2019	93	19	35	21
2020	33	16	56	11
Total	366	112	163	100

1202. An agreement on the information exchange on money laundering, predicate offenses and the financing of terrorism is not mandatory according to the legislation of the Republic of Uzbekistan; that is the actual interaction with the FIUs of foreign states can be carried out without such agreement. As the analysis shows, in recent years, almost 40% of requests were sent to the FIUs of 42 foreign countries that do not have bilateral legal bases for cooperation in the field of information exchange with the FIU of Uzbekistan (Latvia, Czech Republic, USA, Germany, Azerbaijan, Lithuania, Tajikistan, Austria, Luxembourg, Malaysia, etc.).

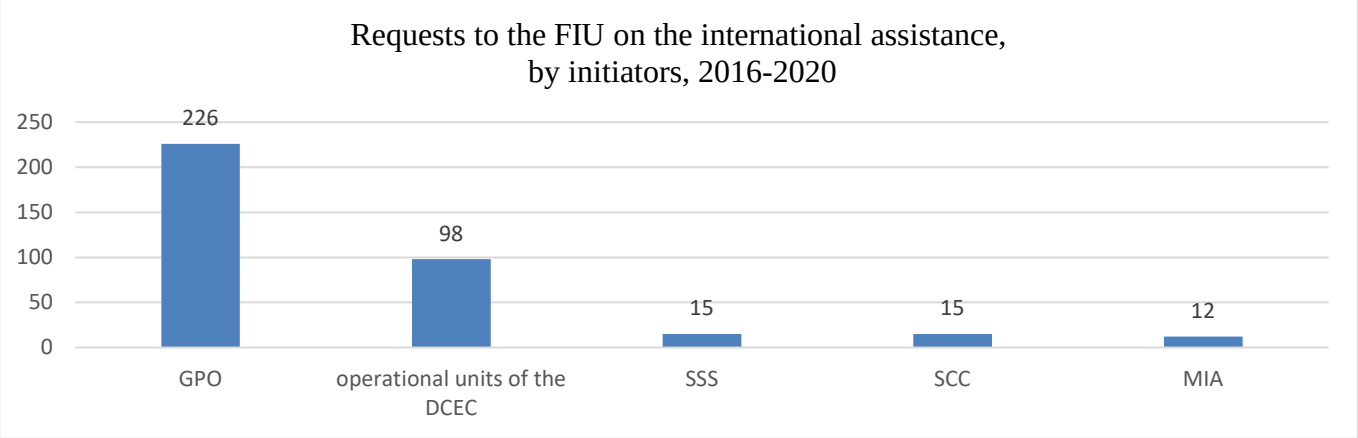
1203. The most active information exchange in ML issues in the years 2016-2020 corresponds to the directions of financial flows of the Republic of Uzbekistan, reflecting export and import directions, and it was carried out with the FIU of Russia, Kazakhstan, Kyrgyzstan, China, Latvia, Turkey, USA, and Germany.

Chart 2.1. Top countries receiving FIU requests (ML-related).



1204. All LEAs are aware of the opportunities of the DCEC in terms of international cooperation through the FIU and use these opportunities for information exchange, as necessary. In 2016-2020, 73% of the sent ML-related requests were initiated by the SSS, the MIA, and the investigative units of the Prosecutor's Office, the remaining 27% were initiated by the operational units and the inquiry of the DCEC. These statistics show that the LEAs understand these opportunities of the FIU and use them in practice.

Chart 2.2. Requests by initiators (ML and TF)



Case study 2.9. (International cooperation through the FIU)

JV Company Invest LLC borrowed $2.5 million from a commercial bank, at a preferential interest rate for the purpose of modernization of the technological line for textile production. The company pledged the plant building and facilities as collateral.
After that, JV Company Invest LLC entered into 2 import contracts for a total of $ 2.5 million, with Offshore shell LP and Offshore invest LP, registered in the country of A., for the supply of equipment for the textile industry and spare parts.
Under the above contracts, $500 million was transferred to the account of Offshore shell LP, opened with the Bank offshore, and $2 million was transferred to the account of Offshore invest LP, opened with the same bank.
Upon the expiration of the contract, the foreign partners did not supply the textile equipment, which led to the insolvency of JV Company Invest LLC regarding the bank loan.
One of the founders of the JV Company Invest LLC named Arsen submitted a statement to the regional prosecutor's office, claiming that the co-founder, Assad and the director, Mukhtar, by prior conspiracy and without the knowledge of Arsen, drew up fictitious documents on pledging the plant building and facilities as collateral security, borrowed a loan and embezzled borrowed funds by transferring money to unknown accounts opened in the offshore jurisdiction.
Within the framework of this criminal case, a request was sent to the DCEC, in order to establish the following:

- the BO of Offshore shell LP and Offshore invest LP, as well as their possible connection with the suspect Assad and Mukhtar;
- the further flow of funds subject to arrest;
- the circle of persons possibly involved in the criminal case;
- signs of money laundering for further criminal prosecution.

While examining this request, the DCEC sent an international request to the FIU of country A. According to the information received, the beneficiary of the accounts was the applicant Arsen, and the funds were transferred to his personal accounts. After the receiving of the information by the prosecutor's office, an international wanted list was announced against Arsen, Assad and Mukhtar.
The collateral agreement remained in force and the collateral was transferred to the assets of a commercial bank.

Effective interaction between the DCEC and the prosecutor's office facilitated the disclosure of information about the BO of the offshore company accounts and allowed the investigation to reveal the true essence of the criminal scheme and to prevent the resale of the plant by invalidating the pledge agreement and to seize assets with further confiscation in favor of the bank, thereby preventing criminal proceeds to be transferred abroad.

1205. All requests sent contain details to identify the officer in charge, who can later be addressed directly and clarify necessary questions. The presence of the relevant information in the request is mandatory in accordance with the established forms for the implementation of information exchange through the channels of the Egmont group.

1206. In accordance with the guidelines of the Egmont Group, after the registration of an international request, the DCEC sends a notification to the initiator confirming the receipt of the request, indicating the registration number and contact details of the officer in charge of this request.

1207. There were no cases of refusal to provide information through the channels of the Egmont group. In a number of cases, an informative response to the request could not be given because the persons implied in the request had no connection with the country to which the request had been sent. In such cases, the reasons for sending the request were demanded.

1208. As for the spontaneous information exchange through the FIU, this work is being carried out less actively. The geography of spontaneous information exchange is generally similar to the geography of requests, which is also due to both the directions of financial flows and the ML risks in general. The topics are connected, first of all, with financial transactions of dubious nature.

Table 2.14. Statistics of spontaneous information exchange through the FIU

Year	Sent	Received
	ML	ML
2016		6
2017		11
2018	1	33
2019	15	14
2020	1	26
Total	17	90

1209. Spontaneous information exchange through the FIU was sporadic. In 2020, spontaneous information was sent 3 times: times to the Republic of Tajikistan and 1 time to the Russian Federation. In view of the fact that, in accordance with the NRA, as a rule, TF activities were carried out by convicted citizens of Uzbekistan outside the country, the assessors believe that the country should pay more attention to this issue.

Case study 2.10. (Sending spontaneous information by the FIU to its partners)
The DCEC received an STR from a commercial bank, stating that a citizen of country A, Mrs. Alla opened with the bank a deposit account to which she deposited $75 thousand in cash and instructed to transfer these funds to the settlement account of Estate LLP (UK) for the purchase of the real estate. When the bank carried out proper due diligence of the client, she submitted a passenger customs declaration for the export of $300 thousand and €600 thousand in cash from country B, refusing to disclose the sources of origin of this money.
Commercial banks refused to carry out the operation and Mrs. Alla left the country declaring this amount. The DCEC, having examined this message, did not establish a connection between these funds and a criminal act, and also did not receive information about a crime from the country of origin.
But concurrently, spontaneous information was sent to the FIU of country A, of which Mrs. Alla was a citizen. The FIU of country A forwarded this information to law enforcement agencies for the purpose of conducting a financial investigation.

1210. According to the information received by the Secretariat on international cooperation, such countries as Russia, Turkey, and Germany comment on a positive experience of interaction with the Republic of Uzbekistan through the FIU. The requests received are fulfilled on time, which is facilitated, among other things, by the fact that the DCEC is a law enforcement agency.

1211. The DCEC interacts with foreign FIUs in accordance with the "Procedure for the interaction and information exchange of the DCEC with the competent authorities of foreign states in the field of combating money laundering, predicate offenses, financing of terrorism and financing the proliferation of weapons of mass destruction" (approved by order of the Head of the DCEC dated 03.07.2020 No. 14).

1212. According to clause 16 of this Procedure, a request or spontaneous information received from the competent authorities of foreign states shall be fulfilled as a matter of priority in cases listed below: if the request is related to the financing of terrorism; if it is associated with crimes that have been assigned a very high and high level of risk based on the results of a national risk assessment; if it is associated with the identification or tracking of funds or other assets on an especially large scale; if it is marked "Urgent" and "Very urgent". This practice testifies to a risk-oriented approach to the implementation of international cooperation.

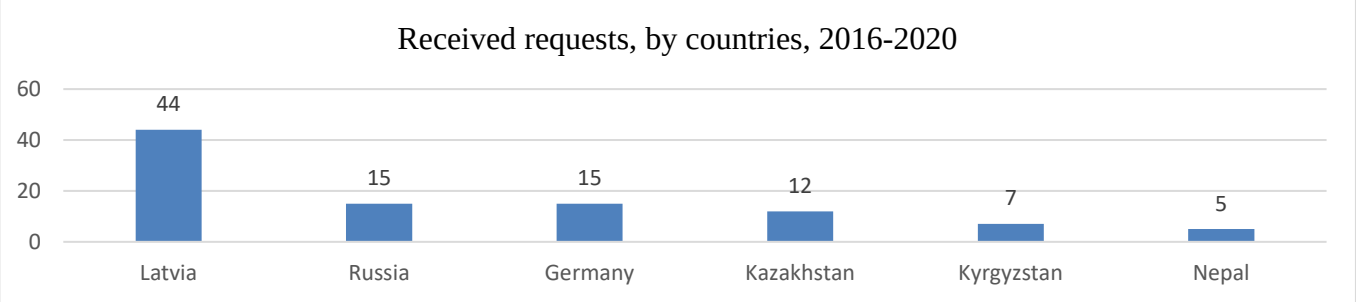
1213. If clarifying questions are made in order to ensure the quality fulfillment of the received requests, the authorized officers of the DCEC interact with officers of the competent authorities of foreign countries by videoconferencing or telephone conversations.

1214. As shows the analysis of the requests received in recent years, almost 50% of the requests received by the DCEC were sent from the FIU of 39 foreign countries that do not have a bilateral legal basis for cooperation on the information exchange with the FIU of Uzbekistan (Latvia, Czech Republic, USA, Germany, Lithuania, Tajikistan, Austria, Luxembourg, Malaysia, etc.), which reflects the active position of the FIU in the implementation of international cooperation.

1215. As with outgoing requests, the geographic scope of incoming requests is relevant and reflects the country's risk profile (corruption and economic crimes), as illustrated by the example of jurisdictions that sent the highest number of requests in 2016-2020.

1216. The deadlines for the fulfillment of requests are stipulated by bilateral and multilateral international treaties. The fulfillment of the received requests is provided, as a rule, within a period of up to one month. According to the analysis of the terms of fulfillment of international requests received in the period of 2016-2020, the DCEC fulfilled more than 80% of the requests within 30 days, and in response to the remaining 20%, interim responses were sent based on the available information. Also, after receiving the necessary information that had been requested from the relevant institutions of the republic, additional responses were sent in order to fulfill the request thoroughly and with high quality.

Chart 2.3



1217. When information is received from foreign FIUs (both spontaneous messages and requests), financial investigations are carried out, and the resulting information is sent to other foreign FIUs.

Case Study 2.11. (Spontaneous information from the FIU of a foreign state)
The DCEC received spontaneous information from the FIU of a Central European state regarding individual entrepreneurs “I.” and "K.", as well as LLC "WL".
According to the information received, in the period from November 27, 2017, to May 25, 2018, funds in the total amount of USD 1.3 million were received on the account of company “WT”, including:
- USD 606.9 thousand from individual entrepreneur "I.",
- USD 148.8 thousand from individual entrepreneur "K.",
- USD 576.8 thousand from LLC "WL".
Then these funds were immediately transferred to foreign accounts. These transactions had no apparent economic sense and were of a transit nature.
Following the results of a financial investigation, the DCEC established that LLC "WL" was registered in an offshore zone and the beneficiaries were foreign citizens "M." and "T.".
It was also established that LLC "WL" failed to surrender timber import proceeds in the amount of 17.5 billion soums, which resulted in tax evasion in the amount of 877.4 million soums.
As a result of OIM, a criminal case was initiated against the director of LLC "WL" under Art. 184, 189 of the CC.
Due to the fact that the beneficiaries of foreign company "WT" were foreign citizens, and the entrepreneurs' funds were transferred as payment for timber at the request of the foreign partner, the DCEC sent spontaneous information to the FIU of the native country of these citizens. Feedback was received about the ongoing investigation, and the foreign FIU requested permission to transfer the information to the LEA.

1218. The DCEC may refuse a foreign FIU to fulfil the request in the cases listed below:

- if its fulfillment threatens the national security of the Republic of Uzbekistan or contradicts the international obligations of the Republic of Uzbekistan;
- it does not comply with the Principles for the exchange of information between FIUs of the Egmont Group (that is, the request is not associated with the country, it contains no description of the circumstances of the criminal actions, etc.),

1219. However, there are no such facts.

Law enforcement authorities

1220. LEAs pay due attention to the use of other forms of international cooperation and are able to effectively apply them to their activities. Other assistance within international cooperation includes sharing of experience and training of officers, the exchange of current information with foreign colleagues, and expert support in criminal cases.

1221. The National Central Bureau (NCB) of Interpol under the MIA provides law enforcement agencies with information from databases on the registration of vehicles and on results of cross-border checks of foreign citizens and stateless persons and of the check held at the registering on the territory of the Republic of Uzbekistan for the purpose of possible identifying criminals put on the international wanted list, including the search in stolen and lost passports database. Only a part of this information exchange is related to ML/TF. At the same time, members of the FATF Global Network presented cases confirming the importance and value of the information provided by the competent authorities of the country.

Table 2.15. The number of requests sent and received through the NCB of Interpol channels

	2016	2017	2018	2019	2020
Received	498	809	2590	2001	2029
Sent	799	1408	2069	1913	1395

1222. The country's LEAs, as part of their communication via Interpol, also request information on ML-related assets, as well as data needed to investigate ML predicate offences, including corruption and tax crimes.

1223. In the past few years, the MIA of the Republic of Uzbekistan has concluded Cooperation Agreements with the MIAs of the CIS states. The concluded agreements imply the possibility of sending a request for assistance in obtaining information on the committed crimes and on the persons involved. Thus, within the framework of international cooperation, the MIA also receives data from the Main Information and Analytical Center of the MIA of Russia.

1224. The GPO interacts with foreign colleagues at the ARIN-WCP site, a regional group similar to CARIN. At the same time, it is not entirely clear to what extent the competent authorities use the capabilities of this network for the purpose of tracing assets. The number of requests sent through Interpol and the nature of the information requested, together with the small usage of MLA capabilities for tracing assets, indicate that there are opportunities to expand the range of information to be received. It would be useful for Uzbekistan to participate in the UNODC Stolen Asset Recovery Initiative (StAR) and the Interpol Global Focal Point Network on Asset Recovery.

1225. The MIA also participates in the work of the Bureau for the Coordination of Combating Organized Crime (BKBOP CIS) and the Central Asian Regional Information Coordination Center for Combating Illicit Trafficking of Narcotic Drugs, Psychotropic Substances and Their Precursors (CARICC).

1226. The GPO participates in the work of the Coordination Council of General Prosecutors of the CIS states. In addition, the GPO has concluded more than 25 interagency Agreements and Memorandums with the competent authorities of foreign states on the information exchange in the field of combating crime.

1227. The SSS interacts with colleagues within the framework of the Anti-Terrorism Center of the CIS States (ATC CIS), the Regional Anti-Terrorist Structure of the Shanghai Cooperation Organization (RATS SCO), the Conference of Special Services of Turkic-Speaking States (The Turkic Council), and also holds bilateral meetings for the exchange of the crucial investigative information. For example, during the meetings held in 2019 in Tashkent and Nur-Sultan, the Kazakhstan side received and transmitted information on the financial capabilities of international terrorist organizations and radical extremist organizations, their financing channels, as well as the existing connections between terrorist groups.

Table 2.16. Statistics of international meetings held by the SSS

	2016	2017	2018	2019	2020
At the level of the SSS Direction	8	7	6	7	2
At the level of experts	16	15	13	17	3

Table 2.17. Statistics of bilateral meetings held by the SSS

	2016	2017	2018	2019	2020
At the level of the SSS Direction	14	16	17	15	17
At the level of experts	42	53	62	47	11

1228. The SSS also actively exchanges information on TF combating with foreign colleagues. Thus, for the period 2016-2020, 3750 messages concerning combating terrorism were transmitted (of which 111 messages were on TF), and 2510 messages on combating terrorism were received, of which 63 concerned TF. The effectiveness of information exchange is confirmed by positive results. Thus, as a result of such cooperation, 19 terrorist attacks on the territory of the CIS states were prevented, also 255 persons were detained due to the transmitted information, and 529 persons involved were deported to Uzbekistan.

1229. If necessary, law enforcement agencies use diagonal cooperation, in order to find experts and to exchange other valuable information.

Case study 2.12. (Forensic examination with the participation of an invited foreign expert)
An art criticism examination of the painting by Rembrandt became necessary for the investigation of the criminal case conducted by the GPO. For the purpose of this examination, an expert commission was established with the assistance of the Ministry of Culture of the Republic of Uzbekistan, and an expert from the Russian Federation was invited to participate. An official trip to the Republic of Uzbekistan was organized for the expert. The expert's opinion based on the results of the examination served as evidence in the criminal case.

1230. The presented data show that LEAs are more likely to seek for other forms of international cooperation and provide cooperation when requested.

SCC

1231. Customs authorities cooperate with 37 countries subject to 137 bilateral international agreements on cooperation and mutual assistance in customs affairs. On June 22, 2021, the SCC and the Federal Customs Service of the Russian Federation signed an agreement on AML/CFT issues and a memorandum on the prevention, detection and suppression of dubious financial transactions by parties involved in foreign economic activity.

1232. SCC has Order No. 26 dated 25.01.2019 "On the approval of the instructions on the procedure for the conduct of office work and the execution of documents in the customs authorities"; automated information systems for document management and customs control have been developed and implemented, which systems allow to control the timing of execution, priority, maintenance and interaction both at the interagency and international levels.

1233. International cooperation includes the information exchange, including the exchange of investigative information, the organization and conduct of joint OIM. The main partners are the Federal Customs Service of the Russian Federation, the Ministry of Finance of the Republic of Kazakhstan, and the State Customs Committee of the Republic of Belarus. The main categories of international requests are as follows: verification of documents, comparison of the value of goods, tracking of the movement of goods, and verification of legal persons and their characteristics.

1234. The SCC does not keep separate statistics on the exchange of information on ML/TF issues, but at meetings, the assessors were acquainted with examples of interaction, which show the efficiency and high quality of information exchange.

Table 2.18. Statistics of international cooperation through SCC

Year	Requests sent	Responses received	Requests received	Responses sent
2016	144	81	207	207

2017	114	77	161	161
2018	357	230	202	202
2019	585	352	127	127
2020	580	201	16	16

Supervisory bodies

1235. Supervisory bodies for FIs are parties to international agreements and participate in other relevant international organizations, so there are no legislative impediments to the exchange of relevant information. Uzbekistan (first ACMD, now – MF) has been a member of the International Organization of Securities Commissions (IOSCO) since August 2014. The Antimonopoly Committee takes part in the work of the Interstate Council on Antimonopoly Policy. The Central Bank cooperates and exchanges information related to the implementation of supervisory functions, including in the field of AML/CFT, with international organizations, central banks, and other foreign bodies of banking supervision and monetary policy. The Central Bank has concluded five agreements on cooperation and information exchange, including on AML/CFT issues, with regulators of the Russian Federation, the Republic of Kazakhstan, the Republic of Korea, the United Arab Emirates, and the Arab Republic of Egypt. + Georgia, Turkey

1236. The actual AML/CFT interaction is carried out only by the Central Bank. In 2019, the Central Bank sent 4 requests and received 1 request. The requests concern obtaining additional information on dubious transactions (the nature of the organization's activities, the geography of cash flows), as well as identifying the BO or recipients of payment.

1237. Taking into account the existence of other channels for the exchange of investigative information on AML/CFT issues (for example, the FIU) and the limited integration of the Republic of Uzbekistan into the international financial system, the assessors consider the current level of interaction between the supervisory authorities to be adequate.

Providing other forms international cooperation for AML/CFT purposes

1238. According to the FIU, information for the purpose of identifying BO is requested and provided in the overwhelming majority of requests. However, there are no specific statistics on such requests (see Case Study 2.9).

1239. The LEAs reported that so far they have not received requests to establish the BO of legal persons that are residents of the Republic of Uzbekistan. The assessors believe that there are no impediments in the country to the collection and provision of relevant information under the MLA procedures. Firstly, foreign partners who provided feedback for the survey of the FATF Global Network, have not reported of cases when the Republic of Uzbekistan refused to provide such information or could not provide it. Secondly, in the legislation of the Republic of Uzbekistan, there are no prohibitions or other regulatory impediments to the transfer of such information to foreign colleagues, and the necessary legal basis has also been established for the collection of such information.

1240. In the period of 2016-2019, the STC did not receive or send requests within international cooperation, which implies the exchange of basic information and information on the BO of legal persons and formations. In 2020, the STC received 6 requests from the Kyrgyz Republic, 1 request from the Republic of Kazakhstan, and 22 requests from the Federal Tax Service of the Russian Federation regarding the payment or non-payment of VAT by some Uzbekistan companies when importing goods from these countries. The STC took appropriate measures to collect the information specified in the requests, and no non-payment was detected.

1241. Taking into account the above issues, even in the absence of relevant practice, all competent authorities are able to receive and transmit information on BO through MLA channels.

1242. At the same time, meetings with representatives of the competent authorities did not testify that they had a unified understanding of the plan of action when working with relevant requests. It appears that the value of the information on the beneficiaries transmitted by the country will largely be determined

by the circumstances of a particular case, including the competence of a particular officer in charge of the fulfillment of such a request at all its stages, including quality control.

1243. The GPO provided examples of effective actions for tracing, seizing, and recovering assets (see IO.8). However, the establishing of BO is not a priority in investigating predicate offenses with the transnational component. It should be noted that the low activity of international cooperation in the identification of BO is also associated with the fact that most of the facts of ML in the Republic of Uzbekistan are self-laundering and occur on the territory of the country.

1244. Despite the fact that law enforcement agencies are staffed with qualified and well-trained specialists, the team of assessors made a point on the necessity of systematic advanced professional training in identifying BO in cross-border crimes.

Overall conclusions on IO.2

1245. The Republic of Uzbekistan provides constructive and timely MLA and extradition. However, feedback is not requested on a regular basis. The competent authorities confidently use the MLA mechanism in cases under investigation. In general, the scope and nature of the requested legal assistance correspond to the risk profile of the country. However, the competent authorities could have paid more attention to exploring the transnational element. Extradition is actively requested, successfully in most cases. However, more attention should be paid to the existing cases of rejection of extradition requests. MLA mechanisms are used to trace, seize and recover assets. In most cases, the measures taken lead to asset seizure and recovery, but this work should be continued.

1246. LEAs effectively cooperate and exchange information on various international platforms. Such cooperation leads to substantial practical results. Understanding the method for identifying beneficiaries in the framework of international cooperation is not fully satisfactory.

1247. The country can provide information on BO, but not all agencies have a sufficient understanding of the algorithm for identifying beneficiaries as part of international cooperation.

1248. Information exchange through the FIU is carried out perpetually, together with a wide range of partners, and its nature corresponds to the national ML/TF risks. Representatives of the FIU demonstrated various instruments and channels of international interaction that can cover not only the needs of financial intelligence itself but also of other LEAs. The country needs to pay more attention to this channel of interaction during financial investigations by the DCEC itself and by other LEAs. Statistics of incoming and outgoing requests and spontaneous messages demonstrate Uzbekistan's moderate level of information search through the FIU channels. Also, the conclusion can be drawn of the insufficient usage of the incoming information due to the small number of positive examples of its use.

1249. There is little international supervisory cooperation compared to international law enforcement or FIU cooperation, but this is due to the lack of information exchange needs of supervisory authorities due to the specific nature of the sectors.

1250. **The Republic of Uzbekistan is rated as having a substantial level of effectiveness for IO.2.**

ANNEX A. TECHNICAL COMPLIANCE ANNEX

Recommendation 1 - Assessing risks and applying a risk-based approach

1251. Recommendation 1 was added to the FATF Recommendations in 2012, so compliance with this Recommendation was not analyzed during the first round of EAG mutual evaluations.

Criterion 1.1

1252. The Republic of Uzbekistan conducted NRA in 2019. The public results of the assessment were published on the website of the DCEC. The methodology used to conduct the NRA is based on the FATF Guidance "Risk assessment of money laundering and terrorist financing at the national level" (2013), taking into consideration the ML/TF risk assessment methodologies of the World Bank, International Monetary Fund. The NRA contributed to the identification of the main categories of country ML/TF risks, as well as to the development of further steps to address them.

1253. It establishes the obligation of institutions conducting transactions with monetary funds or other property [108], as well as supervisory bodies, to systematically, at least once a year, conduct identification and analysis of possible ML/TF risks and to take appropriate measures for mitigating the identified risks. ML/TF NRAs and SRAs are governed by the Decree of the President of the Republic of Uzbekistan No. PP-3947 of September 20, 2018 (cl. 1, 4, 6) and the Regulation on the Interagency AML/CFT/CPF Commission (cl. 4, 5, 13).

Criterion 1.2

1254. The AML/CFT Law stipulates that the coordination of measures aimed at assessing the ML/TF risks is carried out by a specially authorized state body (Article 7-1). This body is the DCEC, which coordinates the conduct of NRA and actions of AML/CFT/CPF bodies (paragraphs 5, 6 of subclause 5 of clause 11 of the Regulation on the DCEC (Annex 1 to the Decree of the President of the Republic of Uzbekistan of 23.05.2018, No. UP-5446)). Moreover, for the purpose of conducting NRA and improving the national AML/CFT policy, an Interagency AML/CFT/CPF Commission was established (Presidential Decree PP-3947-son of 20.09.2018).

Criterion 1.3

1255. The authorities and organizations are obliged to update ML/TF risks at annual intervals (Article 7-1 of the AML/CFT Law).

Criterion 1.4

1256. The NRA results must be provided to all authorities involved in AML/CFT and to institutions conducting transactions with monetary funds or other property not later than 3 days after their approval (cl. 7-1 of the AML/CFT Law). The obligation to provide the NRA results is also stipulated by cl. 74 of the "Methodology of ML/TF risk assessment at the national level in the Republic of Uzbekistan" (approved by the decision of the IAC of 17.09.2019, Minutes No. 3). The public part of the NRA is published on the Internet portals of the Republic of Uzbekistan competent authorities[109].

1257. Mechanisms of provision of the NRA results (open and closed communication channels, workshops and training) are established by the Order of the Head of the DCEC (Order No. 35 of 28.06.2021).

Criterion 1.5

1258. Provision is made for risk-based AML/CFT measures: measures applied to prevent or reduce ML and TF must be consistent with the identified risks and allow taking a decision to apply enhanced or simplified control measures and effective allocation of resources (Art. 7-1 of the AML/CFT Law).

---

[108] In Uzbek legislation, the requirements refer to the institutions conducting transactions with monetary funds or other property. This notion includes FIs and DNFBPs in FAFT definition and some other institutions (lottery organisers, etc.)

[109] http://new-department.uz/ru/press/news/439/

1259. In accordance with the Presidential Decree of 28.06.2021 (No. UP-6252 of 28.06.2021), the development strategy of the national AML/CFT/CPF system of the Republic of Uzbekistan was approved, which contains a detailed action plan for dealing with the identified threats and risks. This decree amended the documents regulating the organizational and staff activities of the DCEC (No. UP-5019, updated). The SSS and the SCC prepared internal closed documents (expert assessors are familiarized with them) to minimize the identified risks based on the 2020 NRA results. In May 2021, a joint instruction of the General Prosecutor, the Chairman of the SSS, the Minister of Internal Affairs and the Chairman of the SCC on the procedure for studying the financial aspects of criminal activity in the process of OIA, pre-investigation check, inquiries and preliminary investigations was adopted.

1260. As part of the fight of the STC against shadow economy and tax offences, the Decree of the President of the Republic of Uzbekistan "On organizational measures to reduce shadow economy and increase the efficiency of tax authorities" No. UP-6098 of 30.10.2020 and Resolution of the Cabinet of Ministers "On the management of tax risks, identifying taxpayers (tax agents) with tax risks, as well as the organization and conduct of tax audits" PKM No. 1 of 07.01.2021 were approved.

1261. The CB, as well as some supervisory bodies (Ministry for Development of Information Technologies, Antimonopoly Committee), approved action plans for mitigating the identified risks by internal orders.

Criterion 1.6

1262. The legislation of Uzbekistan does not provide for exceptions for FI or DNFBPs from the requirements to apply certain FATF Recommendations.

Criterion 1.7

1263. Uzbek legislation establishes measures aimed at responding by the AML/CFT regime if a higher risk is identified. Article 15 of the AML/CFT Law provides for the obligation of reporting entities to take measures to mitigate the identified risks.

1264. The requirements to ICR for all FIs and DNFBPs also oblige organizations to assess ML/TF risks by the customer profile, geography and type of transactions and apply appropriate enhanced measures to control the identified risks[110].

Criterion 1.8

1265. The legislation of Uzbekistan does not provide for the application of simplified procedures, except for the legislative permission given to some of the FIs and the auditors' sector not to conduct CDD procedures in relation to the state government bodies.[111]

Criterion 1.9

1266. Supervisors are required to ensure that FIs and DNFBPs fulfil their responsibilities under Recommendation 1. All sectors of FIs and DNFBPs have an AML/CFT supervisor. For all FIs and DNFBPs, the AML/CFT supervisory, licensing and registration authorities or the DCEC shall develop and approve the ICRs.

Criterion 1.10

a) FIs and DNFBPs are required to document their risk assessments. This is established in their ICRs .[112]

---

[110] cl. 54-58 of Resolution No. 2886 of 23.05.2017, cl. 39-42 of Resolution No. 2925 of 04.09.2017, cl. 16-2, 23-2, 23-3, 23-4 of Resolution No. 2036 of 03.11.2009, cl. 33-37 of Resolutions No. 3061 of 28.08.2018, cl. 16, 23-1 – 23-3 of Resolution No. 2020 of 19.10.2009, cl. 17-2 – 17-5 of Resolution No. 2034 of 03.11.2009, cl. 13, 18-1 – 18-3 of Resolution No. 2033 of 03.11.2009, cl. 16, 26-29 of Resolution No. 2038 of 06.11.2009, cl. 13-1, 19-1 – 19-3 of Resolution No. 2265 of 22.09.2011, cl. 14, 20-2, 20-3 of Resolution No. 2257 of 24.08.2011, cl. 29-32 of Resolution No. 3101 of 15.12.2018, cl. 14-2, 21-1 – 21-3 of Resolution No. 2037 of 05.11.2009.

[111] cl. 31 of Resolution No. 2886 of 23.05.2017, cl. 29 of Resolution No. 2925 of 04.09.2017, cl. 22-3 of Resolution No. 2036 of 03.11.2009, cl. 29 of Resolution No.3061 of 28.08.2018, cl. 27 of Resolution No. 3101 of 15.12.2018.

[112] cl. 54 of Resolution No. 2886 of 23.05.2017, cl. 39 of Resolution No. 2925 of 04.09.2017, cl. 23-1 of Resolution No. 2036 of 03.11.2009, cl. 12 of Resolution No. 3061 of 28.08.2018, cl. 23-1 of Resolution No. 2020 of 19.10.2009, cl. 13 Resolution No. 3101 of 15.12.2018, cl. 17-3 of Resolution No. 2034 of 03.11.2009, cl. 18-1 of Resolution No. 2033 of 03.11.2009, cl. 25 of Resolution No. 2038 of 06.11.2009, cl. 19-1 of Resolution No. 2265 of 22.09.2011, cl. 20-1 of Resolution No. 2257 of 24.08.2011, cl. 21-1 of Resolution No. 2037 of 05.11.2009

b) The ICR of reporting entities established the obligation for organizations and their officials to consider customers on the basis of geographical, operational criteria and assess the risk level of transactions conducted by customers to assess their own risks and submit risk assessment reports to the authorized body.[113]

c) The FIs and DNFBPs are required to keep these assessments up-to-date.[114]

d) The ICR stipulates the obligation to provide information on risk assessment to competent authorities.[115] In addition to the requirement in the ICRs to provide information about risks to supervisory authorities, mechanisms (systems) for transmitting such information via electronic communication channels have been established in practice. The sector of the payment system operators has no explicit obligation to provide information on the results of risk assessment.

Criterion 1.11

1267. Article 15 of the AML/CFT Law provides for the obligation of reporting entities to take measures to identify risks, document the results of the examination and take appropriate measures to mitigate the identified risks. The ICR of reporting entities, which are approved by supervisory bodies together with the AML/CFT authorized body, include the criteria and indicators that indicate an increased customer or transaction risk.

a) FIs and DNFBPs are required to develop ICR or internal control programs approved by the senior management of FIs or DNFBPs in order to manage and mitigate risks both identified by the country, and those identified by the particular institution.[116] For a number of sectors (insurance companies, notaries and lawyers, dealers in precious metals and stones, leasing, realtors, lotteries) there are no requirements to develop internal policies/measures approved by the senior management for management purposes and to mitigate the identified risks.

b) FIs and DNFBPs are required to monitor the effectiveness of the internal control implementation and to strengthen measures as necessary[117].

c) The requirements to internal control rules for all FIs and DNFBPs also oblige organizations to assess ML/TF risks by the customer profile, geography and type of transactions and apply appropriate enhanced measures to control the identified risks.[118]

Criterion 1.12

1268. The legislation of Uzbekistan does not provide for the application of simplified procedures.

---

[113] cl. 54 of Resolution No. 2886 of 23.05.2017, cl. 39 of Resolution No. 2925 of 04.09.2017, cl. 23-1 of Resolution No.2036 of 03.11.2009, cl. 33 of Resolution No. 3061 of 28.08.2018, cl. 23-1 of Resolution No. 2020 of 19.10.2009, cl. 29 of Resolution No. 3101 of 15.12.2018, cl. 17-3 of Resolution No. 2034 of 03.11.2009, cl. 18-1 of Resolution No. 2033 of 03.11.2009, cl. 25 of Resolution No. 2038 of 06.11.2009, cl. 19-1 of Resolution No. 2265 of 22.09.2011, cl. 20-1 of Resolution No. 2257 of 24.08.2011, cl. 21-1 of Resolution No. 2037 of 05.11.2009.

[114] cl. 54 of Resolution No. 2886 of 23.05.2017, cl. 39 of Resolution No. 2925 of 04.09.2017, cl. 23-1 of Resolution No. 2036 of 03.11.2009, cl. 66 of Resolution No. 3061 of 28.08.2018, cl. 23-1 of Resolution No. 2020 of 19.10.2009, cl. 53 Resolution No. 3101 of 15.12.2018, cl. 17-3 of Resolution No. 2034 of 03.11.2009, cl. 18-1 of Resolution No. 2033 of 03.11.2009, cl. 25 of Resolution No. 2038 of 06.11.2009, cl. 19-1 of Resolution No. 2265 of 22.09.2011, cl. 20-1 of Resolution No. 2257 of 24.08.2011, cl. 21-1 of Resolution No. 2037 of 05.11.2009.

[115] cl. 54 of Resolution No. 2886 of 23.05.2017, cl. 39 of Resolution No. 2925 of 04.09.2017, cl. 23-1 of Resolution No. 2036 of 03.11.2009, cl. 33 of Resolution No. 3061 of 28.08.2018, cl. 23-1 of Resolution No.2020 of 19.10.2009, cl. 17-3 of Resolution No.2034 of 03.11.2009, cl. 18-1 of Resolution No.2033 of 03.11.2009, cl. 25 of Resolution No.2038 of 06.11.2009, cl. 19-1 of Resolution No.2265 of 22.09.2011, cl. 20-1 of Resolution No.2257 of 24.08.2011, cl. 21-1 of Resolution No.2037 of 05.11.2009

[116] cl. 6, 54 of Resolution No. 2886 of 23.05.2017, cl. 6 of Resolution No. 2925 of 04.09.2017, cl. 13 of Resolution No. 3061 of 28.08.2018, cl. 6, 7 of Resolution No. 2033 of 03.11.2009, cl. 6 of Resolution No. 2038 of 06.11.2009, cl. 14 of Resolution No. 3101 of 15.12.2018

[117] cl.99 of Resolution No.2886 of 23.05.2017, cl.74 of Resolution No.2925 of 04.09.2017, cl.68 of Resolution No.3061 of 28.08.2018, cl.8 of Resolution No.2257 от 24.08.2011, cl.11 of Resolution No.2038 of 06.11.2009, cl.34-2 of Resolution No.2020 of 19.10.2009, cl.66 of Resolution No.3266 of 30.06.2020, cl.1, 14 of Resolution No.3309 of 09.06.2021, cl.14-1 of Resolution No.3101 of 15.12.2018, cl.29-1 of Resolution No.2265 of 02.09.2011, cl.34-1 of Resolution No.2036 of 03.11.2009, cl.28-2 of Resolution No.2033 of 03.11.2009, cl.27-2 of Resolution No.2034 of 03.11.2009, cl.14 of Resolution No.3310 of 17.06.2021, cl.11 of Resolution No.3101 of 15.12.2018.

[118] cl. 54-58 of Resolution No. 2886 of 23.05.2017, cl. 39-42 of Resolution No. 2925 of 04.09.2017, cl. 16-2, 23-2, 23-3, 23-4 of Resolution No. 2036 of 03.11.2009, cl. 33-37 Resolution No. 3061 of 28.08.2018, cl. 16, 23-1 - 23-3 of Resolution No. 2020 of 19.10.2009, cl. 17-2 - 17-5 of Resolution No. 2034 of 03.11.2009, cl. 13, 18-1 - 18-3 of Resolution No. 2033 of 03.11.2009, cl. 16, 26-29 of Resolution No. 2038 of 06.11.2009, cl. 13-1, 19-1 - 19-3 of Resolution No. 2265 of 22.09.2011, cl. 14, 20-2, 20-3 of Resolution No. 2257 of 24.08.2011, cl. 29-32 of Resolution No. 3101 of 15.12.2018, cl. 14-2, 21-1 - 21-3 of Resolution No. 2037 of 05.11.2009.

Weighting and Conclusion

1269. The Republic of Uzbekistan has a good legal framework for managing and mitigating ML/TF risks on the part of both government bodies and the private sector. However, the sector of the payment system operators does not have a requirement to provide information on the results of the risk assessment to the competent authority.

1270. **Recommendation 1 is rated Largely Compliant.**

Recommendation 2 - National cooperation and coordination

1271. In the 2010 mutual evaluation report, the Republic of Uzbekistan was rated under Recommendation 31 as "LC". The main deficiencies were related to the lack of transparency of the cooperation mechanisms of the Coordinating Council and interagency agreements, which did not allow a full assessment of the effectiveness of the measures taken.

Criterion 2.1

1272. By Presidential Decree No. UP-6252 of 28.06.2021, based on the results of the NRA the National AML/CFT/CPF Strategy of the Republic of Uzbekistan was approved. This document defines the national AML/CFT/CPF policy, approves the Roadmap for taking measures aimed at reducing risks and threats and establishes the obligation to update the risk assessment at least every three years.

Criterion 2.2

1273. In Uzbekistan, DCEC is the specially authorized body, which coordinates the work of and the competent authorities involved in AML/CFT/CPF (Article 9 of the AML/CFT Lawcl. 1 of the Decree, cl. 11 of the Regulation on the DCEC). For the purpose of conducting NRA and improving the national AML/CFT policy, the Interagency AML/CFT/CPF Commission was established (Presidential Decree PP-3947-son of 20.09.2018).

Criterion 2.3

1274. The IAC was established in order to coordinate the functioning of the national AML/CFT/CPF system as well as for the implementation of Recommendation 2, its decisions are binding for all the AML/CFT system participants[119], including LEAs, supervisory and other competent authorities. (cl. 1, 2 of the Regulation approved by Presidential Decree PP-3947-son of 20.09.2018). The IAC consists of the deputy heads of 23 ministries and agencies - LEAs, supervisory and other competent authorities (GPO, SC, CB, MIA, MF, MD, MFA, MJ, MITCD, SCC, STC, Antimonopoly Committee, State Industrial Security Committee, State Assets Management Agency, etc.).

1275. Presidential Decree No. UP-6252 of 28.06.2021 (Annex No. 3) approved the list of ministries and agencies involved in AML/CFT/CPF.

1276. To ensure interaction at the operational level, including information exchange, the decision of the IAC (paragraph 8 of Minutes No. 2 of the meeting of 11.07.2019) approved the composition of the IAC expert working group, which includes employees of all agencies - members of the IAC. The tasks of the expert group include ensuring continuous interagency cooperation on combating money laundering and financing of terrorism at the expert level.

1277. Various mechanisms of interdepartmental interaction, including information exchange, were also established at the operational level. Interagency Mobile Groups (IMG) and the Operations Coordination Group (OCG), which is an interagency coordinating body that includes the SSS, the MIA, the SCC, the FIU, and the National Information and Analytical Center for Drug Control under the Cabinet of Ministers of the Republic of Uzbekistan, have been established. Joint Operational Headquarters (JOH) for combating terrorism and extremism, including their funding, have been

[119] See “Background and Other Contextual Factors” in Chapter 1.

established in all regions of the country as part of the SSS, prosecutors' offices, the MIA and the SCC. The activities of this JOH are regulated by an interdepartmental document of these agencies.

Criterion 2.4

1278. Coordination and cooperation on the issues of countering PF at the highest and operational level are carried out (similar to Criterion 2.3) by the IAC and within the activities of the Expert Group. Within the framework of interaction on CPF issues, a joint resolution of 22.06.2021 No. 25/01/24-2085 of the FIU, CB, Goskomprombez, and SCC was adopted.

1279. Also, there are bilateral confidential agreements (resolutions) on the interaction between the FIU, SCC, MIA, SSS, and STC, which were demonstrated to the assessors during the on-site mission to Uzbekistan. The DCEC has agreements on operational cooperation with other bodies (see R.29).

Criterion 2.5

1280. The AML/CFT Law establishes the obligation of all the AML/CFT/CPF system participants to ensure data protection and confidentiality (Art. 20 of the Law). Such an obligation does not restrict the information exchange between participants.

1281. The DCEC and competent authorities cooperate and share AML/CFT/PFPF information on the basis of interagency agreements, of which there are currently 21. These agreements include clauses establishing the data format, the obligations of the parties to ensure the confidentiality of the information obtained in the framework of information exchange, the prevention of its disclosure or use for other purposes, not provided for in these agreements, as well as and the methods of data transfer. Closed electronic communication channels and special-purpose postal communications are used for data transfer. Besides that, the issues of data protection and confidentiality are included in internal departmental documents.

Weighting and Conclusion

1282. **Recommendation 2 is rated Compliant.**

Recommendation 3 – Money laundering offence

1283. In the last mutual evaluation report, the Republic of Uzbekistan was rated as "Largely Compliant" with regard to the criminalization of the money laundering offence.

1284. The major deficiencies were found to be: (i) the disposition of Article 243 of the CC (ML) does not cover the act of possession or use of property obtained by criminal means, which is one of the elements of ML, in accordance with the Vienna and Palermo Conventions; (ii) the CC does not criminalize such types of established categories of offences as insider deals and market manipulation.

1285. The Republic of Uzbekistan has not amended the wording of Article 243 of the CC since the previous evaluation.

Criterion 3.1

1286. In the Republic of Uzbekistan ML is criminalized in Article 243 of the CC – "Legalization of proceeds from criminal activity". Criminal liability shall be incurred for committing the following acts with money or other assets obtained as a result of criminal activity: (i) giving a legal appearance to the origin of property (money or other assets) through its transfer, transformation or exchange; (ii) concealing or disguising the true nature, source, location, method of disposal, movement, true rights with respect to money or other assets or its ownership. According to cl. 3 of Resolution No. 1 of the Plenum of the SC of 11.02.2011 "On some issues of judicial practice in cases of legalization of criminal proceeds" [120] (hereinafter – Resolution of the Plenum of the SC No. 1), legalization of proceeds means giving by guilty persons a legal appearance to origin of money or other assets

[120] Resolutions of the Plenum of the Supreme Court – acts issued by the Supreme Court, including the clarification of applying the laws, binding on the courts, other bodies, enterprises, institutions, organizations and officials who apply these laws (Law of the Republic of Uzbekistan of 14.12.2000 No. 162-II "On Courts").

obtained as a result of criminal activity bytransfer, conversion or exchange, as well as concealment or disguise of the true nature, source, location, disposition, or movement of genuine rights with respect to money or other property or its ownership. Giving a legal appearance to the origin of money or other property obtained as a result of criminal activity consists, as a rule, of carrying out financial transactions and/or making transactions with such money or property.

1287. The criminalisation of these acts is consistent with the provisions of the Vienna and Palermo Conventions.

1288. In the CC, in accordance with the basic principles of the legal system, the acquisition, possession and use of knowingly criminal property are criminalized as a separate norm in Article 171 of the CC (Acquisition or sale of property obtained by criminal means), which is a predicate offence to the commission of money laundering.

Criterion 3.2

1289. The country considers any offence included in the CC to be a predicate offence to money laundering if it results in obtaining criminal proceeds. All categories of offences under the FATF Recommendations except insider deals and market manipulation are criminalized under criminal law.

Criterion 3.3

1290. The Republic of Uzbekistan does not use a threshold approach to define predicate offences.

Criterion 3.4

1291. The subject matter of the offence under Article 243 of the CC is "monetary funds or other assets". The criminal law of the Republic of Uzbekistan does not define the terms "assets" and "monetary funds". According to Article 169 of the Civil Code and cl. 3 of Resolution of the Plenum of the Supreme Court No. 1, the property shall mean movable and immovable property, including property rights, things, securities, services, results of intellectual activity, including exclusive rights to them (intellectual property), virtual assets (cryptocurrency)[121]. This definition of property correlates with the definition of property in the General Glossary in the FATF Recommendations.

1292. In accordance with Article 3 of the AML/CFT Law the proceeds of crime include (i) profit or benefit received from the use of money or other property obtained by criminal means (proceeds of crime); (ii) property into which the money or property obtained by criminal means was transformed or converted (e.g. construction of real estate from building materials obtained by criminal means); (iii) property obtained through the acquisition of money or other property acquired by criminal means; (iv) property obtained through the use of money or other property obtained by criminal means. In such cases, the property shall be recognized as criminally obtained only in the part corresponding to the amount of money or value of the acquired property, virtual assets (cryptocurrency).

1293. The value of the laundered property is irrelevant to liability under Article 243 of the CC. However, the size of legalization (significant, large or especially large) of such property according to cl. 8 of Resolution of the Plenum of the Supreme Court No. 1, determines the term of punishment.

Criterion 3.5

1294. Criminal legislation of the Republic of Uzbekistan does not contain imperative norms requiring mandatory conviction of a person for a predicate offence, but it’s necessary to establish the fact of the criminal origin of the legalized proceeds.

Criterion 3.6

1295. The criminal legislation of the Republic of Uzbekistan, for the purposes of criminal prosecution for ML, considers predicate offences committed outside of the Republic of Uzbekistan as equivalent to those that took place inside the country, provided that they are criminalized on the territory of Uzbekistan (see Criterion 3.2). Thus, there is a provision for the recognition as committed on the

[121] Virtual assets (cryptocurrency) are included in SC Plenum Resolution No. 1 of July 3, 2020.

territory of the Republic of Uzbekistan of acts which: (i) were committed outside Uzbekistan and the criminal result occurred on the territory of Uzbekistan; (ii) were committed on the territory of Uzbekistan and the criminal result occurred outside of Uzbekistan; (iii) form, together or along with other acts, an offence, part of which was committed on the territory of Uzbekistan (Article 11 of the CC).

1296. Citizens of the Republic of Uzbekistan, as well as stateless persons permanently residing in Uzbekistan may be prosecuted for committing an offence outside the country if they have not been punished in the country where the act was committed (Article 12 of the CC).

Criterion 3.7

1297. The application of the ML offence to persons who have committed predicate offences (see Criterion 3.2) does not contradict the fundamental principles of national legislation. According to the CC, such a combination of predicate acts on ML is a set of offences (Article 33).

Criterion 3.8

1298. Conclusions about the intent to commit an offence and the knowledge of its commission can be made on the basis of available evidence and the established factual circumstances of the case (Articles 81 and 82 of the CC).

1299. Resolution of the Plenum of the Supreme Court No. 1 specifies various examples of factual circumstances of a criminal case indicating that the perpetrator had the intent (cl. 6).

Criterion 3.9

1300. Article 243 of the CC provides for a penalty for laundering proceeds of the offence of five (5) to ten (10) years' imprisonment. The offence is categorized as a serious offence. There are no other penalties for committing the offence.

1301. According to cl. 8 of Resolution of the Plenum of the Supreme Court No. 1, in determining the amount of the punishment the courts must take into consideration the value of the laundered property as well as other circumstances set forth in Resolution of the Plenum of the Supreme Court No. 1 of 03.02.2006 "On Practice of Imposing Punishment by Courts".

1302. Appointment of a milder punishment, which is not provided for in the Article, is possible only in exceptional cases in the presence of circumstances that significantly reduce the degree of public danger of the committed offence (Article 57 of the CC).

1303. The sanctions for predicate crimes similar in purpose to money laundering (e.g. tax evasion, customs violations, illegal entrepreneurial activity, acquisition or sale of criminally derived property, etc.) include fines, correctional work and restriction of freedom, with a maximum prison sentence of 5 years for these offences (customs violations - 8 years)

1304. According to the CC, the liability for predicate crimes (theft, fraud, bribery, etc.) is increased depending on the size of the caused property damage or criminal income, for the definition of which the three-link system - significant, large and especially large amount of damage - is applied[122].

1305. For instance, fraud on a large scale is punished with 3 to 5 years of imprisonment and on an especially large scale with 8 to 10 years of imprisonment. For large-scale bribery, the penalty is 5 to 10 years imprisonment, and for especially large-scale bribery, it is 10 to 15 years imprisonment.

1306. However, there is no gradation of liability for ML offences depending on the amount of property legalised. In addition, there is no increased liability if the ML offence is committed repeatedly by a person who has previously committed terrorist offences or by a person using his or her official position.

[122] For the purposes of criminal law (determining the amount of fine, damage, criminal income), in Uzbekistan, they use the reference settlement value (RSV), an indicator determined by Presidential Decree.
According to Section 8 of the CC, a significant amount of damage (criminal proceeds) ranges from 100 to 300 RSV (from USD 2,300 to USD 6,900 at the exchange rate as of 02.07.2021; a large amount - from USD 6,900 to USD 11,500; an especially large amount - over USD 11,500).

1307. The sanction of Article 243 of the CC is dissuasive, but it is not proportional (coherent).

Criterion 3.10

1308. The legislation of the Republic of Uzbekistan provides for several forms of liability for the commission of offences: criminal, administrative, civil, etc.

1309. In the Republic of Uzbekistan, criminal liability for legal persons is not established, since, in accordance with the fundamental principles of law, only individuals are subject to criminal liability (Article 17 of the CC).

1310. Administrative liability of legal persons is not stipulated by the legislation of the Republic of Uzbekistan.

1311. According to Article 53 of the Civil Code, a legal entity may be liquidated by a court decision in case of carrying out activities prohibited by law, which include, among others, laundering of criminal proceeds.

1312. Obviously, the liquidation of legal persons by way of civil proceedings does not prevent individuals from being held criminally liable for ML.

1313. The lack of variability of sanctions in relation to legal persons for ML makes it impossible to conclude that they are coherent and dissuasive in nature.

Criterion 3.11

1314. The CC provides for the criminalization of all necessary forms of participation in an offence. Liability for participation in an offence (co-perpetration, organization, instigation, aiding and abetting, assisting and advising, preliminary agreement, uniting in an organized group or criminal community) is stipulated by Articles 28 and 29 of the CC. Preparation and attempt to commit an offence are punishable under Article 25 of the CC.

1315. Criminal liability for participation in an offence or for an incomplete offence is incurred under Article 243 of the CC with reference, respectively, to Articles 28, 29 or 25 of the CC for purposes of qualification and determination of the term of punishment. At the same time, the maximum term of punishment for the preparation and attempted commission of ML can not exceed 7 years and 6 months of imprisonment, except in cases of committing ML by a particularly dangerous recidivist, organized group or criminal association (Article 58 of the CC).

1316. The failure to pledge unauthorized assistance to a person who has committed money laundering is criminalized in Article 241 of the CC (Failure to report an offence or its concealment).

Weighting and Conclusion

1317. Insider deals and market manipulation, which are included in the established categories of offences in accordance with the FATF Recommendations, are not criminalized in the Republic of Uzbekistan.

1318. The sanction of Article 243 of the CC with respect to individuals is not proportional (coherent), and sanctions with respect to legal persons are limited to only one type of liability.

1319. **Recommendation 3 is rated Largely Compliant.**

Recommendation 4 - Confiscation and provisional measures

1320. According to the results of the first round of mutual evaluation, the Republic of Uzbekistan was rated as "LC" under the former Recommendation 3. As a deficiency, the experts noted the impossibility to analyze in detail the powers of the Republic of Uzbekistan competent authorities in terms of searching for property, which is or may be subject to confiscation, as these powers are provided for in the documents of limited circulation.

Criterion 4.1

1321. The legislation of the Republic of Uzbekistan considers confiscation to be the uncompensated seizure of property from the owner by a court decision for the commission of an offence or other offence (Art. 204 of the Civil Code). The criminal law does not contain provisions regulating the institution

of confiscation. Since confiscation is not defined by criminal law as a punishment or other measure of legal influence applied by the court for the commission of an offence, it is not regarded as a direct legal consequence of a criminal act. The procedure for the application of confiscation of property is governed by the rules of the CPC.

1322. This conclusion is also supported by the fact that, by Article 487 of the CPC, the court's failure to apply the confiscation of criminal assets is not regarded as a substantive violation of the law of criminal procedure and does not entail a quashing or amendment of the judgment by the higher courts.

a) Confiscation of legalized (laundered) property: The property that was the object of the offence, if it cannot be returned to the previous owner, shall be returned to the State under a court sentence (Art. 284 of the CPC). Similar provisions are stipulated by Art. 211(5) of the CPC.

According to the explanations contained in cl. 2 of Resolution of the Plenum of the SC of 11.02.2011 No.1 "On some issues of judicial practice in cases of legalization of criminal proceeds" (as amended by Resolution of the Plenum of the SC of 03.07.2020 No. 12) the subject matter of an ML offence is monetary funds and other property obtained as a result of the commission of an offence (see criterion 3.2), as well as any profit or benefit received from the use of such property, as well as converted or transformed in whole or in part into other property or attached to property acquired from legal sources.

Property derived from the legalization of proceeds is the subject matter of an ML offence and on the basis of Article 204 of the Civil Code is subject to confiscation after compensation for material damage caused to a natural or legal person. Thus, confiscation applies to legalized (laundered) property, but the priority issue is compensation for the damage.

b) Proceeds from predicate offences (including proceeds or other profits derived from such proceeds): the CPC provides a mechanism for confiscation of proceeds and other profits from predicate offences (see Criterion 3.2). Thus, according to Article 285 of the CPC, money, items of property and other valuables acquired by the accused with funds obtained by criminal means are spent on compensation for the property damage caused (confiscation of property directly obtained by criminal means), and the amount exceeding this damage is returned to the State (confiscation of profits) by court sentence). In the absence of damage or its full compensation property, money and other valuables acquired after the commission of criminal acts with the funds gained by criminal means, by a court verdict shall be transferred to the state (Resolution of the Plenum of the SC of 13.12.2012 № 17 "On some issues of application of legislation on physical evidence in criminal cases".

If property obtained by criminal means is sold by the perpetrator to third parties who are bona fide purchasers, seized from them and returned to their possession, the court verdict shall transfer the money, items of property and other values received by the defendant from the sale of this property to the State (profit confiscation).

At the same time, Article 288 of the CPC provides for the possibility of leaving the property obtained as a result of the crime (the subject of the crime) in the ownership of the guilty if the victim rejects this property and the court satisfies the victim's civil claim for compensation of its value.

Funds used or those planned to be used for ML or the commission of predicate offences: Objects specially designed, manufactured or adapted for the preparation or commission of an offence as well as property used directly in the process of committing an offence to achieve criminal goals are instruments of offence and are recognized as physical evidence (Articles 203-1, 207 of the CPC). In accordance with Article 211, cl. 1, of the CPC, instruments of offence belonging to the perpetrator are subject to confiscation and are to be transferred to the competent institutions for the execution of the decision on confiscation or are destroyed. Property that does not belong to the perpetrator is returned to the legal owners, and if no such owners are identified, they are transferred to the state’s revenue.

c) Property that is the proceeds of, or intended for use for, TF, terrorist acts or terrorist organizations: The above provisions of the CPC apply equally to TF offences (see sub-criterion (b)). Besides that,

Article 29 of Law No. 167-II of 15.12.2000 "On Combating Terrorism" provides for confiscation, on the basis of a court decision, of the property of an organization recognized as terrorist.

d) Property of corresponding value: The law of criminal procedure provides for the confiscation of property of corresponding value. Thus, according to Art. 284 of the CPC, property that was the object of an offence, if it cannot be returned to the previous owner, will be returned to the State by court order. If this property is not found, a court verdict or, in case of termination of a criminal case, a court decision issued by way of civil proceedings will result in the recovery of its value to the state's revenue.

Criterion 4.2

a) Identification, tracing and assessment of property subject to confiscation: Identification and tracing of property subject to confiscation prior to initiation of a criminal case may be carried out within the framework of criminal intelligence and detective operations by carrying out such investigative measures as interviews, inquiries, collecting samples for comparative analysis, test purchase, examination of objects and documents, operational surveillance, inspection of residential and other premises, buildings, structures, locations and means of transportation, etc. (Art. 12,14 of the Law of the Republic of Uzbekistan "On operational investigative activity" of 25.12.2012 No. LRU-344).

When criminal proceedings are initiated, the identification of property liable to confiscation is carried out through investigative operations such as seizure (Art. 157 of the CPC), searches (Art. 158, 161 and 162 of the CPC), and examinations of the scene of events, locations, premises, objects and documents (Art. 135-141 of the CPC).

According to the Law "On Bank Secrecy" (LRU №530-II of 30.08.2003) the bodies carrying out ORD, bodies of prosecution, investigation and inquiry, the court may obtain information on transactions, accounts and deposits of clients. In addition, in order to identify the property subject to confiscation, LEAs may request and receive information from the databases of other state bodies, including the FIU (for more details see R.31).

The procedure for an appraisal is provided for the property that is seized in the course of criminal prosecution. According to Art. 293 of the CPC, such appraisal is carried out by the investigator, the inquirer, at market prices existing at the time of appraisal, considering wear and tear, and, where necessary, with the participation of a specialist or appraisal organizations. Money, bonds, checks, shares, and other securities shall be recorded at face value.

b) Provisional measures: According to Art. 9 of the AML/CFT/PF Law, the DCEC, if there are sufficient grounds, sends orders to suspend for a period not exceeding thirty business days a transaction in monetary funds or other assets in order to implement measures to counter ML/TF/PF.

In accordance with UP-5446, dated May 23, 2018, the FIU is granted to suspend and/or freeze funds and other assets of persons suspected of economic crimes, ML, FT and PF.

Accordingly, the suspension of transactions in monetary funds or other assets and freezing can be applied for the purposes of criminal proceedings in a limited category of criminal cases.

According to Article 290 of the CPC, in order to execute a sentence in terms of a civil action, other property penalties, which by virtue of the provisions of the law include confiscation of property, the inquirer, investigator, or court must seize the property of the suspect, accused, and civil defendant (persons who are financially responsible for the perpetrators under the law). The seizure extends throughout the period of the preliminary investigation and the trial until the final judgment is handed down by the court.

The seizure is also imposed on the property recognized as physical evidence, in order to prevent its appropriation, embezzlement, concealment, destruction or damage.

The seizure is not imposed on the house, apartment, home furnishings and other objects necessary for the normal viability of the family of the guilty person and civil defendant, a list of which is approved by Resolution of the CM of 14.04.2009 No.110. However, proceeding from the explanations stated in cl. 2 of the Resolution of the Plenum of the SC of 13.12.2012 No. 17 "On certain issues of application of the

law on material evidence in criminal cases" the property, money and other valuables acquired after the criminal actions with the funds gained illegally or obtained as a result of the crime are considered material evidence. Thus, interim measures set out in Article 207 of the CPC may be applied to property that is not subject to seizure due to restrictions imposed by law but which is material evidence in the case. Such property may be attached to the criminal case file or deposited in the prescribed manner.

Residential and non-residential premises, regardless of their form of ownership, may be seized in cases of their use to commit treason, terrorism, sabotage, encroachment on the constitutional order, the President of the Republic of Uzbekistan, including when these offences are combined with other grave and especially grave offences (which include ML and TF offences).

Seizure of property is carried out by the competent authorities without prior notice. Seizure of property as a provisional measure is based solely on criminal procedural mechanisms and cannot be carried out before a criminal case is initiated.

There are no mechanisms (except for economic) for applying provisional measures to prevent transactions with the property subject to confiscation prior to the initiation of a criminal case for predicate offences.

c) Prevention of the possibility of non-application of provisional measures: pursuant to Art. 290 of the CPC, when the property is seized, the owner (possessor) is prohibited from disposing of it and, where necessary, prohibited from using it.

The property (as a rule - prohibited for circulation) may also be seized and deposited with other persons (whose competence includes the execution of the decision in terms of confiscation).

In the case of leaving the seized property in custody, the person is explained the statutory responsibility for the safety of this property and a corresponding receipt is taken.

Illegal disposal of seized property entails criminal liability under Art. 233 of the CC.

In order to prevent the loss, damage or deterioration of property recognized as material evidence in a case, such property shall be attached to the case file or transferred for safekeeping in accordance with the established procedure, thus ensuring its safety until the final procedural decision on the case is taken.

d) Application of appropriate investigative measures: Seizure of property shall be imposed by order of the inquirer or investigator with the authorization of the prosecutor or by order of the court, which has the right to entrust the conduct of this investigative action to the investigative body.

In urgent cases, property may be seized without the prosecutor's authorization, but with subsequent notification and justification of the decision in the procedural documents.

If the inquirer or investigator does not take measures to seize the property, they may be obliged to do so by the court in which the criminal case is pending.

The CPC contains a detailed regulation of the procedure for the seizure of property (Art. 290-294 of the CPC). At the same time, there is no norm of direct action in the CPC, which provides for the possibility of seizure of property of third parties, i.e. nominal owners. At the same time, according to the amendments made to the Resolution of the Plenum of the SC No. 26 dated 27.12.2016 (by the Resolution of the Plenum of the SC No. 23 dated 10.06.2021) seizure may be imposed on the property of the suspect or accused, which is held by third parties if sufficient grounds to believe that the property actually belongs to the suspect or the accused are obtained in the course of the proceedings.

Criterion 4.3

1323. Pursuant to Art. 285 of the CPC, when property obtained by criminal means is seized from a bona fide purchaser and returned to the owner, the purchaser has the right to sue the convicted person in civil proceedings for compensation for the harm caused by the seizure of the property.

1324. According to the above provisions of the law (Art. 285 of the CPC), damage caused to a bona fide purchaser as a result of the seizure of property obtained by another person by criminal means is not direct damage from an offence and is not subject to compensation in the framework of criminal proceedings.

1325. In addition, a third party whose property was seized during the proceedings on the grounds that it actually belonged to the suspect or the accused, have the right to apply to the court for releasing the property from seizure by way of civil proceedings. However, as follows from Art. 116 paragraph 4 of the CPC, a civil case concerning such an action may not be considered until the court has taken a final procedural decision in the criminal case during which the property of the third party has been seized.

1326. Protection of the rights of bona fide third parties is provided by the CPC, which grants them the right to appeal a court sentence in the part that affects their rights and interests.

1327. However, referring bona fide purchasers' claims to the sphere of civil proceedings means imposing on them the burden of proof in civil proceedings and entails an expenditure of material resources in the form of payment of state duty for filing a claim. In addition, the decision on the civil claim may be taken only after the criminal case is considered on the merits, which increases the period during which a good faith purchaser cannot dispose of its property.

Criterion 4.4

1328. The procedure for confiscation, sale or destruction of property to be transferred to the State on the basis of court decisions in criminal and administrative cases, decisions of investigative authorities in termination of the proceedings regarding instruments of offence, material evidence, decisions of tax and customs authorities is specified in Regulation of July 15, 2009 No. 200 approved by the CM.

1329. This Regulation regulates in detail the issues of seizure and sale of cash and non-cash funds, securities, other types of movable and immovable property, and the procedure for the destruction of property.

1330. However, only the possibility of transferring property for safekeeping to persons (organizations), which are obliged to observe and ensure appropriate storage conditions for spoilage, damage, embezzlement or misappropriation of property, can be attributed to the management mechanisms. Legal acts regulating other management mechanisms, including complex assets, are not provided to assessors.

1331. The procedure for seizure and sale of crypto-assets is regulated in the annex to the joint resolution of the GPO, the MIA, the SSS and the SCC of 21.05.2021. According to the mentioned interdepartmental act, digital devices, crypto-wallets, manuscripts and notes may be seized, examined and recognized as physical evidence in order to detect the circulation of crypto-assets. Crypto-assets are subject to seizure pending clarification of their origin and (or) adjudication. Seizure is carried out by transferring crypto-assets to a crypto-wallet of a law enforcement agency. In this case, the value of crypto-assets is determined at the time of seizure according to the quotations of crypto-exchanges, for non-convertible - according to the prices on service platforms. Confiscation and circulation of crypto-assets to the state property are carried out in accordance with the procedure established by law by means of exchange (sale).

Weighting and Conclusion

1332. The Republic of Uzbekistan does not criminalize insider deals and market manipulation (see Recommendation 3, criterion 3.2), which excludes the application of confiscation of proceeds obtained as a result of these offences.

1333. Seizure of property as a provisional measure and confiscation of property in Uzbekistan is based solely on criminal procedural mechanisms.

1334. **Recommendation 4 is rated Largely Compliant.**

Recommendation 5 - Terrorist financing offence

1335. In the 2010 MER, the Republic of Uzbekistan was rated under SR II as "LC". The lack of criminalization of acts of seizure, theft and use of nuclear materials, as well as illegal actions against fixed platforms located on the continental shelf, was noted as the main factors which influenced the rating under this recommendation.

1336. Following the previous evaluation, The Republic of Uzbekistan introduced amendments to the Law of the Republic of Uzbekistan of 15.12.2000 No. 167-II "On Combating Terrorism" in terms of the definition of "terrorist activity", "terrorist act", "terrorism", "terrorist", "terrorist financing", as well as corresponding amendments to the CC (Law of 25.04.2016 No. LRU-405).

Criterion 5.1

1337. In the Republic of Uzbekistan TF is criminalized based on the UN Convention for the Suppression of the Financing of Terrorism as a separate corpus delicti under Article 155-3 of the CC. Any activity aimed at (1) ensuring the existence, functioning, and financing of a terrorist organization, (2) ensuring travel abroad or movement through the territory of the Republic of Uzbekistan to participate in terrorist activities, (3) preparation and performance of a terroristic action, (4) direct or indirect (i.e. through intermediaries) providing or collecting any funds, resources, other services (a) to terrorist organizations or (b) persons assisting or participating in terrorist activities is punishable under criminal law.

1338. The notion of "terroristic action" is contained in Article 2 of Law of 15.12.2000 No. 167-II and covers all the acts provided for in Article 2(1) of the UN Convention for the Suppression of the Financing of Terrorism.

Criterion 5.2

1339. Under the provisions of Article 155-3 of the Criminal Code, intentional provision or collection of any funds, resources or other services to terrorist organizations or individual terrorists ("persons assisting or participating in terrorist activities") is criminalized. The criminal law provides for liability for such actions regardless of the means by which they are collected or provided. Both direct and indirect terrorist financing are covered by this offence.

1340. According to Article 155-3 of the CC, TF crime is defined as terroristic activities financing. This notion is provided for in paragraph 10 of Article 2 of Law No. 167-II of 15.12.2000 and includes carrying out a terrorist act. Thus, the country's criminal law criminalises the provision and collection of funds for a terrorist act.

1341. According to Article 155-3 of the CC, TF crime includes financing of the terrorist organization defined as a stable association of two or more persons or terrorist groups for carrying out terrorist activities (para 7 of Article 2 of Law of 15.12.2000 No. 167-II). However, the decision to recognize an organization as a terrorist organization is made by a court outside the criminal process (Article 29 of the same Law). Based on the principle of direct application of international law (Article 3 of Law of 15.12.2000 No. 167-II), including terrorist organisations in the UN sanction list equates to the decision of the national court. Thus, the financing of a de facto terrorist organisation that has not been recognised by Uzbekistan's court or has not been included in the UN sanctions list (e.g. financing of newly created organisations in Uzbekistan or organisations recognised as terroristic in other states) is not criminalised.

1342. According to paragraph 6 of Article 2 of Law of 15.02.2000 No. 167-II, a terrorist group is a group of persons that have committed a terrorist act, the preparation of a terrorist act or an attempt to commit a terrorist act by prior conspiracy.

Criterion 5.2bis

1343. Article 155-3 of the CC establishes liability for any activity aimed at financing travel abroad or movement through the territory of the Republic of Uzbekistan for participating in terrorist activities.

1344. According to Article 2 of Law of 15.12.2000 No. 167-II, terrorist activity is defined as activity that includes organizing, planning, preparing and committing a terroristic action, incitement of commting a terroristic action. The terrorist activity also includes establishing a terrorist organization, recruiting, training and arming terrorists, their financing and logistical support, i.e. actions carried out by active participants in a terrorist organizationю The actions of persons intending to attend terrorist training do not constitute terrorist activity. Therefore, providing funds to a person to pay for travel for such training would not constitute TF.

1345. Thus, the disposition of Article 155-3 covers possible terrorist purposes of travel outside the country except financing of persons' travelling for their terrorist training. This aspect is connected with the context of the country's risks, as there have been instances of Uzbek nationals travelling abroad for terrorist training in the past.

Criterion 5.3

1346. Article 155-3 of the CC makes no distinction between legitimate or illegitimate sources of funds, resources and other services provided or collected for the purpose of financing terrorist activities. TF is criminalized by the use of "any" funds, resources and services.

Criterion 5.4

1347. The construction of the disposition of Article 155-3 of the CC does not require that the funds were actually used to commit or attempt to commit a terrorist act or were related to a specific terrorist act.

Criterion 5.5

1348. The CPC of the Republic of Uzbekistan does not contain restrictions on the use of evidence collected in the case to support the conclusions of the investigation and the court about the presence of the subjective side of the offence under Article 155-3 of the CC in the actions of a person. De jure it allows the concept of proving a person's intent through his actual actions to be used in court.

Criterion 5.6

1349. Proportionate (coherent) and dissuasive criminal sanctions apply to natural persons convicted of TF.

1350. The CC provides punishment for TF under part 1 of Article 155-3 from 8 to 10 years' imprisonment and is categorized as a grave offence. The qualified corpus delicti of Part 2 of Article 155-3 of the Criminal Code, if the offence was committed repeatedly, by an organized group, a public official or a dangerous recidivist, provides for a punishment of 10 to 15 years' imprisonment and falls under the category of especially grave offences.

1351. Part 3 of Article 155-3 of the Criminal Code provides the basis for exemption from criminal liability of a person who has participated in the financing of terrorism, if he/she has timely warned the authorities or otherwise actively contributed to the prevention of the grave consequences and the implementation of the terrorists' goals.

Criterion 5.7

1352. The Republic of Uzbekistan does not provide for criminal liability for legal persons, since, in accordance with the fundamental principles of law, only natural persons are subject to criminal liability (Article 17 of the CC).

1353. Administrative liability of legal persons is not stipulated by the legislation of the Republic of Uzbekistan.

1354. According to Article 53 of the Civil Code, a legal person may be liquidated by the court decision in case of carrying out activities prohibited by law, including TF. Thus, the legislation of the Republic of Uzbekistan provides for the possibility of bringing a legal person to civil liability. In accordance with Article 29 of the Law of 15.12.2000 No. 167-II, the legal persons recognized as terrorist organizations are subject to liquidation on the basis of a court decision. The property of the liquidated organizations is subject to confiscation. However, provisions of the Law of 15.12.2000 No. 167-II can not be applied to legal persons that carry out legal activities and are not terrorist organizations, but in case a natural person who controls and manages them commits a TF offence on behalf of such an organisation.

1355. Liquidation of legal persons by way of civil proceedings does not prevent natural persons from being held criminally liable for TF.

1356. The lack of variability of sanctions in relation to legal persons for terrorist financing does not allow to conclude that they are proportionate. The dissuasive nature of such sanctions is not explicit, as it depends on the amount of the legal entity's assets.

Criterion 5.8

1357. Uzbekistan's criminal legislation recognises crimes:

a) Preparation and attempt to commit an offence (Artice 25 of the CC).

b) Participation as an accomplice in a TF offence or attempted offence, including intermediation (Article 28 of the CC).

c) Organising and inciting to commit a crime (Article 28 of the CC).

d) Repeated commission of TF crime (Article 155-3, para. 2 of the CC), the commission of a crime by an organized group or criminal association, or based on prior conspiracy (Article 29 of the CC).

1358. Criminal liability for participating as an accomplice in an offence or for an incomplete offence is imposed under Article 155-3 of the CC with reference to Articles 28, 29 or 25 of the CC, respectively, for purposes of qualification and determination of the term of punishment.

1359. Besides that, the criminal law of the Republic of Uzbekistan contains provisions on liability for failure to report a reliably known grave and especially grave offence, which includes all the acts provided for in Article 155-3 of the CC, as well as for unauthorized concealment of such an offence.

Criterion 5.9

1360. Since the country considers any offence included in the CC to be predicate offences to ML if criminal proceeds are derived from it, the offence of terrorist financing (Article 155-3 of the CC) is a predicate offence.

Criterion 5.10

1361. In order to prosecute a person for TF, the possible difference in his or her location and the location of the terrorist or terrorist organization, or the place where the terrorist act was committed does not matter, i.e. the financing of terrorist activities carried out outside Uzbekistan is recognized as an offence as if such terrorist acts were carried out in Uzbekistan.

1362. Moreover, the criminal legislation of the Republic of Uzbekistan provides for the recognition as committed on the territory of Uzbekistan of acts which were committed outside of Uzbekistan and the criminal result occurred on its territory; were committed on the territory of Uzbekistan and the criminal result occurred outside of it; form in the aggregate or along with other acts an offence, part of which was committed on the territory of Uzbekistan (Article 11 of the CC).

1363. There is also a provision for criminal liability for committing an offence outside the country if the person has not been punished in the country where the act was committed (Article 12 of the CC).

Weighting and Conclusion

1364. Uzbekistan's legislation does not criminalise the funding of de facto terrorist organisations which have not been recognised by a court decision as such or which are not included in UN sanctions lists.

1365. Providing funds to a person to pay for travel for training is not covered under the TF offence.

1366. Domestic law provides for a legal entity's only form of liability - its liquidation; such a sanction is not always proportionate and dissuasive.

1367. **Recommendation 5 is rated Largely Compliant.**

Recommendation 6 - Targeted financial sanctions related to terrorism and terrorist financing

1368. According to the results of the 2010 MER, the Republic of Uzbekistan was rated as "NC" under SR III due to the non-compliance of the existing regime of suspension of operations with regard to persons designated in the list of terrorists with the requirements of Resolutions 1267 and 1373, as well as Special Recommendation III in general, the lack of necessary mechanisms for consideration and use of information received from foreign States with regard to the subjects of the freezing.

1369. The Republic of Uzbekistan adopted Order of the General Prosecutor of the Republic of Uzbekistan of 30.09.2016 No. 22-B "On Approval of the Regulation "On the Procedure for Suspension of Operations, Freezing of Monetary Funds or Other Assets, Providing Access to the Frozen Assets and Resuming Operations of Persons Designated in the List of Persons Involved or Suspected of Involvement in Terrorist Activities or Proliferation of Weapons of Mass Destruction" (hereinafter - Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B) to eliminate deficiencies.

Criterion 6.1

1370. The mechanism of implementation of TFS is defined in the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B.

a) According to clause 43 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B, bodies involved in combating terrorism[123], in case of identification or receipt of information about a person to be designated in the sanctions lists made by the UNSC committees, file them to the MFA for subsequent submission to the relevant UNSC committee for consideration. However, the legislation does not specify the competent body responsible for submitting proposals on persons/entities to the relevant UNSC Committee. Participation of the MFA in submitting information to the UN is based on its general function to coordinate the activities in the sphere of international relations, including with international organizations. There are no documents (including internal regulations), confirming and specifically defining its responsibility for this area.

b) Identification of persons and groups (organizations) to be designated in the UN sanctions lists is carried out by the bodies involved in combating terrorism in the order provided in the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B. Additionally, the information provided to the MFA should contain as many details as possible, giving reason to believe that the person meets the criteria for designation in the sanctions lists, as defined by the relevant UNSCRs (cl. 44 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

c) Clause 44 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B determines that in deciding whether to submit a proposal to the UN Committee, there must be information giving grounds to believe that a person meets the criteria for designation in the sanctions lists of the UNSC committees i.e. on the basis of "reasonable grounds" and "sufficient grounds". The evidence criteria (evidentiary standard of proof) are listed in clause 6 of the Regulation in General Prosecutor's Order of 30.09.2016 No. 22-B. The possibility of submitting proposals for designation in the UNSC sanctions lists is limited by criteria in the Regulation. The above-mentioned grounds for proposals for designation are not defined solely by the initiation of criminal proceedings.

d) Competent authorities are required by law to follow the procedure and use the standard forms of designation in the sanctions list made by the relevant UNSC Committees under UNSCR No. 1267 (1999), No. 1718 (2006), No. 1988 (2011), No. 1989 (2011), No. 2253 (2015) (cl. 44 of the Regulation in General Prosecutor's Order of 30.09.2016 No. 22-B).

e) The legislation obliges the competent authorities to provide as much information as possible giving grounds to believe that a person/entity meets the criteria for designation in the sanctions lists of the UNSC Committees, as defined by the relevant UNSCRs, as well as the identification of natural and legal persons (cl. 44 of the Regulation in General Prosecutor's Order of 30.09.2016 No. 22-B). Given that the concept of "as much as possible" is general (collective) it seems that it includes providing the background of the case, other supporting information or documents, as well as information on the links between the proposed designee and any person or entity identified at the moment.

Criterion 6.2

1371. Regarding the designations under Resolution 1373:

[123] The Republic of Uzbekistan has defined 9 State bodies engaged in combating terrorism (article 8 of Law No. 167-II of 15 December 2000 on Combating Terrorism).

a) The DCEC is defined as the competent agency responsible for the maintaining of the List and including in it persons participating or suspected of participating in terrorist activities both for domestic initiatives as well as for the verification of grounds and inclusion on requests from other countries (Article 9 of the AML/CFT Law, clause 11.5 of the Regulation on the DCEC).

b) As mentioned above, identified persons are designated in the List, which consists of two sections: international and national. The definition of a person involved or suspected of involvement in terrorist activities is given in clause 1 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B. The identification mechanism for designation in the List (cl. 1 of Chapter 2 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B) applies. The grounds for designation in the List are specified in Criterion 6.1(c) and are overwhelming. Clause 1 of Chapter 6 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B provides a mechanism for consideration of foreign requests to suspend operations and (or) freeze monetary funds or other assets of persons subject to sanctions due to their involvement or suspicion of involvement in terrorist activities.

c) Requests from other states for inclusion in the List should be considered by the DCEC no later than three working days from the date of receipt of information through official channels from the competent authorities of foreign states. The basis for their execution is the recognition by the Republic of Uzbekistan of foreign sentences and requests based on international treaties (not only about MLA) or the principles of reciprocity (cl. 6 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). In order to determine the validity of the request for grounds for designation in the List and the suspension of operations and (or) the freezing of monetary funds or other assets in accordance with the criteria of Resolution 1373 (2001), the legislation provides requirements for foreign requests for their execution. The DCEC assesses the request for compliance with legal requirements and completeness of the information provided, i.e. applies the standards of "reasonable grounds" and "sufficient grounds" (paragraph 38 of the Regulation in Order of the Prosecutor General of 30.09.2016 No. 22-B). Requests that do not meet the legal requirements are to be returned without execution (cl. 37 and 41 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). Request requirements are publicly available, as the General Prosecutor's Order of 30.09.2016 No. 22-B is publicly available on the Internet. Decisions based on foreign requests are not conditional on the existence of criminal proceedings.

d) The basis for designation in the List is listed in clause 6 of Chapter 2 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B. The list of grounds is exhaustive. Such grounds for designation in the national section of the List are based on the initiation of criminal proceedings, with the exception of the availability of an enforceable court decision of the Republic of Uzbekistan to recognize an organization as terrorist and to liquidate it or ban its activities on the territory of the Republic of Uzbekistan.

e) The requirements for the content of the requests filed to foreign States and the procedure for filing them are regulated in clause 2 of Chapter 6 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B, including the obligation to provide as much identification and evidentiary information as possible.

Criterion 6.3

a) The DCEC has the right to request and receive free of charge the information necessary to carry out CFT measures, including from automated information and reference systems and databases (Article 9 of the AML/CFT Law), as well as information constituting a banking secret (Article 8 of the Law of the Republic of Uzbekistan of 30.08.2003 No. 530-II "On Banking Secrecy"). The legislation stipulates the obligation of the competent authorities to provide information necessary for making the List, as well as the authority of the DCEC to request additional information on their own initiative (cl. 7-11 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

b) The NLAs do not contain a requirement to notify persons or entities who have been identified and whose designation in the List (proposal for inclusion) is pending. Consequently, the competent authorities are allowed and they can act unilaterally (ex parte).

Criterion 6.4

1372. Uzbek law does not fully provide for "without delay" application of the TFS, as the inclusion of a person/entity in the international or national section of the List and the subsequent freezing of assets, may take the time not considered "without delay".

1373. In particular, the MFA informs the DCEC and the competent authorities of the Republic of Uzbekistan of the sanctions lists and relevant resolutions as they are received through official channels (point 8 of the Regulation in Order of the Prosecutor General of 30.09.2016 No. 22-B). The DCEC makes amendments and additions to the List no later than 3 working days. Not later than 1 working day, it electronically submits the List to the relevant supervisory, licensing, and registration authorities and posts it on the website (paragraphs 12 and 21 of the Regulation in Order of the Prosecutor General dated 30.09.2016 No. 22-B).

1374. Institutions conducting transactions with monetary funds or other property are obliged to freeze without delay the funds or other assets of the persons included in the List of persons (Article 15 of the Law on ML/TF/TRMF, paragraphs 3, 24, and 25 of the Regulation in the Order of the Prosecutor General of 30.09.2016 No. 22-B).

1375. In respect of designations under Resolution 1373, the competent authorities shall provide information on the designated person/organisation to the DCEC within 3 working days of their receipt or the occurrence of circumstances for inclusion of the person in the national section of the List (paragraph 7 of the Regulation in Order of the Prosecutor General dated 30.09.2016 No. 22-B). The DCEC shall amend and supplement the List within 3 working days, and then not later than 1 working day electronically communicate the List to the relevant supervisory, licensing and registration authorities, as well as post it on its website (paragraphs 12 and 21 of the Regulation in Order of the Prosecutor General of 30.09.2016 No. 22-B).

1376. Requests received from international organisations, or competent authorities of foreign states shall be considered within 2 working days. A decision shall be made to include the person in the List or not (paragraph 38 of the Regulation in Order of the Prosecutor General dated 30.09.2016 No. 22-B).

1377. Thus, the TFS may be applied within both a few hours and up to 4 days.

1378. At the same time, pending the consideration of the nominee's inclusion in the List, a temporary application of financial sanctions is envisaged (the DCEC shall issue an order to suspend operations for up to 30 working days).

Criterion 6.5

a) Institutions conducting transactions with monetary funds or other property[124] are obliged to suspend without delay and without prior notice a transaction, except for transactions to credit the account of a legal entity or an individual, and (or) freeze monetary funds or other assets of the persons designated in the List, The obligation to freeze (suspend operations) monetary funds and other assets is not stipulated for all individuals and legal persons.

b) The transaction in monetary funds or other assets shall be suspended, and the monetary funds or other assets shall be frozen, if (i) all identification data of the customer or one of the parties to the transaction fully coincide with the person designated in the List; (ii) the monetary funds or other assets used for the transaction, fully or partially belongs to the person designated in the List, or the legal entity that participates in the transaction is owned or controlled by the natural or legal person designated in the List (iv) one of the participants in the transaction acts for or on behalf of a person designated in the List (cl. 25 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). However, this regulation does not provide for the freezing (suspension of transactions) without delay (iii) of monetary funds and other assets derived or generated through the use of monetary funds or other assets that are owned (controlled) directly or indirectly by designated persons or entities.

[124] In Uzbek legislation, the requirements refer to the institutions conducting transactions with monetary funds or other property. This notion includes FIs and DNFBPs in FAFT definition and some institutions (lottery organisers, etc.) However, this notion doesn't cover all physical and legal persons without exception.

c) Citizens and legal persons of the Republic of Uzbekistan, foreign citizens and , as well as stateless persons on the territory of the Republic of Uzbekistan are prohibited from providing access directly or indirectly to monetary funds or other assets, material resources, financial and other services to persons designated in the List, as well as persons acting on their behalf (cl. 2 of General Prosecutor's Order of 30.09.2016 No. 22-B, Article 155^3 of the CC).

d) The legislation of the Republic of Uzbekistan provides mechanisms for communicating information on designations to the financial sector and DNFBPs. Such mechanisms do not fully ensure the principle of "without delay" application of the TFS. The DCEC no later than one working day after the approval, modification or amendment of the List is electronically communicated it to the relevant supervisory, licensing and registration authorities, and also posts the List (or its changes and amendments) on the website, where it is available directly to the financial sector and DNFBPs, which are required to download it from the website (paragraph 23 of the Regulation in General Prosecutor's Order No 22-B of 30.09.2016). Financial sector institutions and DNFBPs must check their participants with the List when carrying out all transactions. Supervisory, licensing and registration authorities shall also bring the List to the attention of Institutions conducting transactions with monetary funds or other property no later than one working day (paragraph 21 of the Regulation in General Prosecutor's Order No. 22-B of 30.09.2016). The issuance of mandatory ICR and their timely amendment and supplementation are used by supervisory, licensing and registration authorities as the guidelines for FIs and DNFBPs.

e) The obligation of organizations involved in transactions in monetary funds or other assets to report to the specially authorized state body on the suspension of operations or freezing of assets, or on the prohibited actions of persons, including attempts to commit them, is provided in Articles 14 and 15 of the AML/CFT/PF Law and in cl. 25 and 26 of the Regulation in General Prosecutor's Order of 30.09.2016 No. 22-B, as well as the internal control rules.

f) The legislation does not provide for the protection of professional risk for employees of the FIU, FIs and DNFBPs in connection with their actions to suspend transactions or freeze assets.

Criterion 6.6

a) The de-listing of a person designated in the List on the basis of the sanctions lists made by the UNSC committees or relevant UNSCRs shall be carried out in accordance with the procedure established in the relevant documents (guidelines) of the committees and UNSC resolutions. A person designated in the List on the basis of sanctions lists made by the UNSC committees or his legal heirs, in case of his death, to be de-listed shall apply to the Office of the Ombudsman established by UN Security Council Resolution 1904 (2009) (cl. 15 and 20 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). The appeal procedures are publicly available, as the General Prosecutor's Order of 30.09.2016 No. 22-B is publicly available on the Internet.

b) The Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B defines the grounds for excluding a person from the national List designated on the basis of the UNSCR 1373 (cl. 14 of the Regulation), as well as the mechanism of de-listing (cl. 13). Exclusion of persons from the List is carried out according to the appeals of the bodies that submitted the relevant information for their designation in the List, or by a court decision. An appeal for de-listing is sent to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan no later than three business days from the date of receipt or detection of information serving as grounds for the exclusion of a person from the List. The detailed mechanism of appeal against designation in the national List and the procedure for review is established by clause 3 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B (cl. 16-17). Individuals and, erroneously designated in the List or subject to exclusion from the List, shall apply with a written motivated application to the Department for Combating Economic Crimes under the General Prosecutor's Office of the Republic of Uzbekistan, which no later than three business days shall file the application for review to the relevant competent authority, which provided information for designating the person in the List. The authority that received the application shall review it and make one of the following reasoned decisions: (i) to make a proposal to exclude the person from the List; (ii) to deny the application. Within three business days of receiving

the decision of the relevant body, the Department for Combating Economic Crimes under the General Prosecutor's Office shall notify the applicant of the decision.

c) In case the application is denied, the person has the right to appeal the decision in court (cl. 18 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

d) The Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B provides a procedure for interaction with the UN on de-listing individuals, but does not imply any detailed mechanisms (specifics) for expedited proposals for de-listing by the 1988 Committee in accordance with any applicable guidelines or procedures approved by the 1988 Committee, including the Focal Point mechanism established under UNSCR 1730.

e) NLA do not regulate the obligation and procedures for informing individuals and organizations about the availability of the Office of the UN Ombudsman, according to UNSCRs No. 1904 (2009), No. 1989 (2011) and No. 2083 (2012).

f) The procedure for resumption of transactions and unfreezing of monetary funds or other assets, including the persons in respect of whom a "false positive" occurred, is stipulated in clauses 27-30 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B.

g) Mechanisms for providing information on de-listing and unfreezing to institutions conducting financial transactions and DNFBPs are provided in clauses 22, 23, 29, 33 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B. The information is provided by the DCEC no later than one working day after amending the List.

Criterion 6.7

1379. Persons designated in the List, in order to secure basic living needs, have the right to appeal to an organization involved in transactions in monetary funds or other assets to access the frozen property to (i) pay for food, rent, utilities, medicines, medical products and medical services, taxes, other mandatory and insurance payments, lawyers and legal advice within average market prices, current fees and charges related to the maintenance of bank accounts or property, and (ii) pay extraordinary expenses (cl. 31 of the Regulation in General Prosecutor's Order of 30.09.2016 No. 22-B).

Weighting and Conclusion

1380. The Republic of Uzbekistan has not identified a competent authority responsible for submitting proposals on persons/entities to the relevant UNSC Committee.

1381. The grounds for designation of a person/entity under UNSCR 1373 on the country's initiative (inclusion in the national section of the List) are conditioned by the existence of criminal proceedings, except for a court decision recognising an organisation as a terrorist and its liquidation or forbidding its activities on the territory of the Republic of Uzbekistan.

1382. The principle of "without delay" application of the TFS is not fully ensured.

1383. The obligation to freeze funds (suspend transactions) and other assets are not envisaged for all physical and legal persons without exception.

1384. There is no obligation to freeze without delay funds (suspend transactions) and other assets derived or generated through the use of funds or other assets that are owned (controlled) directly or indirectly by designated persons or entities.

1385. The immediate communication of information on designations to the financial sector and DNFBPs, as well as de-listing and unfreezing of assets, is not fully ensured.

1386. There are no requirements to protect bona fide third parties acting in a good manner.

1387. **Recommendation 6 is rated Partially Compliant.**

Recommendation 7 - Targeted financial sanctions related to proliferation

1388. TFS implementation requirements in relation to the proliferation of weapons of mass destruction were introduced in the FATF Recommendations in 2012, so their implementation was not assessed in the previous round of mutual evaluation of the Republic of Uzbekistan.

Criterion 7.1

1389. Uzbek law does not fully provide for "without delay" application of the TFS, as the inclusion of a person/entity in the List and the subsequent freezing of assets may take the time not considered "without delay".

1390. The mechanism for implementing PF TFS f is defined in the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B.

1391. A specially authorized state body, the DCEC, makes an appropriate List.

1392. The grounds for designation in the List are specified in clause 6 of the Regulation in the General Prosecutor's Order of September 30, 2016 No. 22-B, including being designated in the sanctions Lists made by committees of the UN Security Council, or relevant UNSCRs.

1393. The MFA informs the DCEC about the sanctions lists made by the committees of the UNSC and the relevant UNSCRs as they arrive through official channels (cl. 8 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

1394. The DCEC no later than three business days from the date of receipt of information makes changes and additions to the List, and then no later than one business day file the List in the electronic form to the relevant supervisory, licensing, and registration authorities, and also places it on its website. The above supervisory, licensing and registration authorities, upon receipt of the List, shall bring it to the attention of the relevant organizations involved in transactions in monetary funds or other assets within one business day (cl. 12 and 21 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

1395. FI and DNFBPs are obliged to freeze without delay the funds or other assets of the persons included in the List of persons (Article 15 of the AML/CFT Law, paragraphs 3, 24, and 25 of the Regulation in the Order of the Prosecutor General of 30.09.2016 No. 22-B).

Criterion 7.2

a) Institutions conducting transactions with monetary funds or other property are obliged to suspend without delay and without prior notice a transaction, except for transactions on crediting the account of a legal or natural person, and/or freeze monetary funds or other assets of the persons designated in the list of persons involved or suspected of involvement in the proliferation of weapons of mass destruction, as well as send a suspicious transaction report to the DCEC (cl. 3 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). The obligation to freeze (suspend transactions) monetary funds and other assets is stipulated only for institutions conducting transactions with monetary funds or other property, but not for all natural and legal persons.

b) The transaction in monetary funds or other assets shall be suspended, and monetary funds or other assets shall be frozen, if (i) all identification data of the customer or one of the parties to the transaction fully coincide with the person designated in the List; (ii) monetary funds or other assets used for the transaction fully or partially belong to the person designated in the List, or the legal entity that participates in the transaction is owned or controlled by a natural or legal person designated in the List; (iv) one of the participants in the transaction acts for or on behalf of a person designated in the List (cl. 25 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). However, this regulation does not provide for the freezing (suspension of transactions) (iii) without delay of monetary funds or other assets received or produced through the use of funds or other assets that are owned (controlled) directly or indirectly by designated persons or entities.

c) Citizens of the Republic of Uzbekistan, foreign citizens, as well as stateless persons on the territory of the Republic of Uzbekistan are prohibited from providing access directly or indirectly to monetary funds

or other assets, material resources, financial and other services to persons designated in the List, as well as persons acting on their behalf (cl. 2 of the General Prosecutor's Order of 30.09.2016 No. 22-B).

d) The legislation of the Republic of Uzbekistan provides mechanisms for communicating information on designations to the financial sector and DNFBPs. Such mechanisms do not fully ensure the principle of "without delay" application of the TFS. The DCEC no later than one working day after the approval, modification or amendment of the List is electronically communicated it to the relevant supervisory, licensing and registration authorities, and also posts the List (or its changes and amendments) on the website, where it is available directly to the financial sector and DNFBPs, which are required to download it from the website (paragraph 23 of the Regulation in General Prosecutor's Order No 22-B of 30.09.2016). Financial sector institutions and DNFBPs must check their participants with the List when carrying out all transactions. Supervisory, licensing and registration authorities shall also bring the List to the attention of Institutions conducting transactions with monetary funds or other property no later than one working day (paragraph 21 of the Regulation in General Prosecutor's Order No. 22-B of 30.09.2016). The issuance of mandatory ICR and their timely amendment and supplementation are used by supervisory, licensing, and registration authorities as the guidelines for FIs and DNFBPs.

e) The obligation of organizations involved in transactions in monetary funds or other assets to report to the DCEC on the suspension of transactions or freezing of assets, or on the prohibited actions of persons, including attempts to commit them, is provided in Articles 14 and 15 of the AML/CFT Law and in clauses 25 and 26 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B.

f) The legislation does not provide for the protection of professional risk for employees of the FIU, FIs, and DNFBPs in connection with their actions to suspend transactions or freeze assets.

Criterion 7.3

1396. The DCEC ensures control over the compliance of legal and natural persons with the requirements of AML/CFT/CPF legislation (Article 9 of the AML/CFT Law).

1397. The DCEC together with the relevant supervisory, licensing, and registration authorities monitors and controls the compliance of the organizations involved in transactions in monetary funds or other assets (cl. 45 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

1398. Administrative liability is provided for violations of legislation on combating the financing of proliferation of weapons of mass destruction, including violations by the relevant supervisory, licensing, and registration authorities of the established procedure for monitoring and controlling compliance with internal control rules (Article 179-3 of the CAO).

1399. Where appropriate, officials of a State body may be held criminally liable for deliberate criminal omission or negligence in the performance of the legislation on combating the financing of proliferation of weapons of mass destruction (Articles 207 and 208 of the CC).

Criterion 7.4

a) The de-listing of a person designated in the List on the basis of sanctions lists of the UN Security Council Committees or the relevant UNSCRs shall be carried out in accordance with the procedure established in the relevant documents (guidelines) of the Committees and the UNSCRs. In order to appeal against the decision to designate a person in the International List section of the List, a natural or legal person may submit an appeal to the Contact Center established under UNSCR 1730 (2006) or the Office of the Ombudsman established by UNSCR 1904 (2009), when a person is designated in the List based on sanctions lists compiled by the UN Security Council Committees or the relevant UNSCRs (cl. 20 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). The appeal procedures are publicly available since the General Prosecutor's Order of 30.09.2016 No. 22-B is publicly available on the Internet.

b) The mechanism of resumption of transactions and unfreezing of monetary funds or other assets in cases of de-listing a person or suspension of transactions and freezing of monetary funds or other assets of a person with similar identification data to the person designated in the List ("false positives") are provided by clauses 27-30 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B.

c) Persons designated in the List, in order to secure basic living needs, have the right to apply to an organization involved in transactions in monetary funds or other assets to gain access to frozen assets for (i) payment for food, rent, utility bills, medicinal funds, medical supplies and medical services, taxes, other compulsory and insurance payments, the services of lawyers and legal advice within the average market prices, current payments and fees associated with the maintenance of bank accounts or the maintenance of the property, as well as (ii) for payment of emergency expenses (cl. 31 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

d) Mechanisms for providing information on de-listing and unfreezing to persons involved in financial transactions and DNFBPs are provided in clauses 22, 23, 29, and 33 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B. The information is provided by the DCEC no later than one working day after amending the List.

Criterion 7.5

a) Suspension of operations and freezing of funds is performed with the exception of transactions for crediting funds received to the account of a natural or legal person (cl. 3 and 25 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B). Thus, the replenishment of frozen accounts is carried out without restrictions. At the same time, debit and other transactions on the accounts are stopped.

b) There are no provisions in the normative legal acts for making designated person or entity ane payment due under a contract entered into prior to the listing.

Weighting and Conclusion

1400. In the legislation of the Republic of Uzbekistan, the principle of "without delay" application of the TFS is not fully ensured.

1401. The obligation to freeze funds (suspend transactions) and other assets are not envisaged for all physical and legal persons without exception.

1402. There is no obligation to freeze without delay funds (suspend transactions) and other assets derived or generated through the use of funds or other assets that are owned (controlled) directly or indirectly by designated persons or entities.

1403. The immediate communication of information on designations to the financial sector and DNFBPs, as well as de-listing and unfreezing of assets, is not fully ensured.

1404. There are no requirements to protect bona fide third parties acting in a good manner.

1405. There is an unsettled issue of making payments under a contract entered into prior to the listing.

1406. **Recommendation 7 is rated Partially Compliant.**

Recommendation 8 - Non-profit organizations (NPOs)

1407. In the last mutual evaluation report, the Republic of Uzbekistan received a "Partial Compliance" rating for compliance with the requirements related to NPOs (former SR.VIII). Since the requirements of R.8 have changed significantly since then, the previous analysis is no longer relevant.

1408. The regulatory framework governing the activities of NPOs in the Republic of Uzbekistan includes clause 3 of Chapter 4 of the Civil Code, the Law of the Republic of Uzbekistan of 14.04.1999 No. 763-I "On Non-State Non-Profit Organizations" (hereinafter - the Law on NPOs, Law of 14.04.1999 No. 763-I), other laws as well as other legal acts.

Name of the law	Number and date of adoption
On Guarantees of Activity of Non-State Non-Profit Organizations	No. ZRU-76 of 03.01.2007
On Freedom of Conscience and Religious Organizations	No. 618-I of 01.05.1998
On Trade Unions, Rights and Guarantees of their Activity	No. 638-XII of 02.07.1992
On Public Funds	No. 527-II of 29.08.2003
On Political Parties	No. 337-I of 26.12.1996
On Financing of Political Parties	No. 617-II of 30.04.2004
On Public Associations in the Republic of Uzbekistan	No. 223- XII of 15.02.1991

On Public Control	No. ZRU-474 of 12.04.2018
On Social Partnership	No. ZRU-376 of 25.09.2014
On Charity	No. ZRU-96 of 02.05.2007

1409. The general concept of non-profit organizations is formulated in Article 40 of the Civil Code. NPO is a legal entity that does not have profit as the main purpose of its activity. NPOs can be established in the form of a public association, a public foundation, an institution funded by the owner, as well as in any other form prescribed by the legislative acts. A non-profit organization may engage in entrepreneurial activities within the limits corresponding to its statutory goals.

Criterion 8.1

a) The 2019 NRA has a section dedicated to analysing the NPO sector, identifying NPOs falling within the FATF definition and those at risk of being used for TF purposes. The Justice Ministry (MJ) in 2019 also conducted the SRA of the NPO sector. The NRA and the SOR results concluded that public associations, public foundations, institutions, international NPOs and religious organisations fall under the FATF definition. At the same time, public foundations and religious organisations are classified as NPOs that are subject to mandatory risk mitigation measures. Both of these types of NPOs are assigned a medium risk level. The risks of international NPOs that are not public foundations or religious organisations are more dependent on their sources of funding. Public associations and institutions are less likely to be subject to international standards for CFT because of the purpose of their activities, the nature of their sources, and the limits of ways where their funds and other assets may be used. The grounds for classifying public foundations and religious organisations as high-risk NPOs include: (i) receiving funds from publicly unknown donors in foreign countries; (ii) receiving material resources from unknown sources; and (iii) having sponsors and participants whose activities are linked to regions with low levels of AML/CFT requirements compliance.

   To determine the types of NPOs at risk and the level of risk, both information available with the supervisory authority (amount of funds received by NPOs, information on violations detected in the activities of NPOs) and information available with the FIU (analysis of STRs, etc.) were used. Neither the NRA report nor the SRA contained information on the use of any other sources of information.

b) The NRA and SRA reports do not provide information on the threats posed by terrorist entities to NPOs at risk, or how terrorists exploit public foundations and religious organisations. The SRA report noted that the vulnerabilities of these NPOs included: the ability to receive funds from third parties in cash through charity boxes or other cash bypassing bank accounts; control over the receipt and expenditure of such funds by the public foundations themselves; and the ability to operate under the guise of religious organisations spreading radical teachings that are the ideological basis for terrorist activity.

c) The Republic of Uzbekistan has analysed the adequacy and sufficiency of measures regulating the entire NPO sector in the SRA report and found them to be effective in protecting NPOs from potential abuse for TF purposes (there are over 20 NLAs in total). At the same time, the authorities are not resting on the existing legal framework but are drafting new regulatory acts, in particular the NPO Code, based on the study of best foreign experience and established national law enforcement practice.

d) Reassessment of the NPO sector is carried out by the MJ by updating the SRA and conducting a planned, systematic analysis of accumulated information on NPO activities. No information on the frequency of updating the SRA was provided.

Criterion 8.2

a) The Republic of Uzbekistan has a policy that ensures transparency in the creation and activities of NPOs, providing accountability and integrity. All NPOs are subject to state registration. Despite the fact that there is no single regulatory document to ensure transparency, integrity, and public confidence in the administration and management of NPOs, legal requirements are contained in the legislative acts on charity and public foundations (Laws No. ZRU-96 of 02.05.2007, No. 527-II of 29.08.2003 and No. 763-I of 14.04.1999), Resolution of the Cabinet of Ministers of 09.10.2019 No. 858. For the relevant state bodies, first of all for the Ministry of Justice, NPOs' activities are quite transparent. There are obligations

for beneficiaries to keep records of charitable donations received, to disclose information about charitable donations received within ten days of their receipt in the media, and if available - on their official websites (Article 5^1 of Law of 02.05.2007 No. ZRU-96). Public foundations are obliged to publish annual reports on their activities and conduct annual audits of their activities in accordance with the law (Articles 25 and 33 of Law of 29.08.2003 No. 527-II). From 01.05.2021, a unified interactive portal "shaffofxayriya" ("Transparent Charity") was launched, which allows centralised accumulation and distribution of charitable donations, monitoring of their targeted use, providing automation and transparency of these processes, as well as providing an opportunity for charity providers to trace the use of their funds (shaffofxayriya.uz). Certain strategic conceptual provisions aimed at increasing public awareness, including the activities of NPOs, are provided by the Decree of the President of the Republic of Uzbekistan of 04.10.2019 No. PP-4473 "On additional measures to increase the effectiveness of public control over the ongoing reforms in the socio-economic sphere, as well as the activity of citizens in the implementation of democratic reforms in the country".

b) During 2015-2019, more than 50 workshops and more than 200 outreach activities on compliance with the requirements specified by law for non-state NPOs, in particular on the prevention of extremist and TF operations in their activities were conducted. As a rule, workshops are held on the following topics: "Compliance with laws and constituent documents"; "Prevention of terrorism and extremism and their negative aspects"; "Risks of terrorism and extremism and their methods" and others. The target audience of these seminars are managers, accountants and other representatives of non-profit organizations. The most significant appear to be the sessions aimed at clarifying the requirements of the legislation on the activities of NPOs, on November 12, 2018, and November 24, 2019, held with the participation of NPOs' representatives. No information was provided on events for the donor community or their participation in events for NPOs.

c) The Republic of Uzbekistan has not provided information on cooperation with NPOs to develop and improve methods for identifying and mitigating the risk of TF and related vulnerabilities, although such cooperation may have taken place in the course of the NRA. Representatives of the NPO sector participate in the development of the Code of the Republic of Uzbekistan on non-state NPOs. The legal framework for such cooperation is the Law of the Republic of Uzbekistan of 25.09.2014 No. ZRU-376 "On Social Partnership" and Decree of the President of the Republic of Uzbekistan of 04.05.2018 No. UP-5430 "On measures to radically increase the role of civil society institutions in the democratic renewal of the country", which established the Advisory Council for the development of civil society under the President of the Republic of Uzbekistan and defined its members. The Advisory Council includes representatives of NPOs.

d) The Republic of Uzbekistan has not provided information on the implementation of special programs encouraging NPOs to conduct operations through regulated financial channels. Legal norms that allow providing property, information, advisory, organizational and training support to NPOs (Article 12 of Law of 25.09.2014 No. ZRU-376 and Article 11 of Law of 03.01.2007 No. ZRU-76) can be seen as measures to encourage NPOs to be more transparent, including by conducting operations through regulated financial channels. However, they are general measures to support NPOs, not special programmes.

Criterion 8.3

1410. There are several state authorities involved in the control (monitoring) and supervision of NPOs, as evidenced by the provisions of Resolution of the CM No. 854 of 23.10.2018 governing the procedure for cooperation between such authorities when exercising control (monitoring) and supervision, as well as the legislation governing the powers of such authorities.

1411. The procedure of monitoring conducted by the Ministry of Justice to verify compliance with the law by NPOs is governed by the Regulation on the procedure of monitoring and studying the activities of NPOs by justice authorities approved by Resolution of the CM of 08.08.2018 No. 635.

1412. The registration authority monitors the compliance of the activities of NPOs and separate subdivisions with the statutory objectives and legislation of the Republic of Uzbekistan, and in order to ensure

legality may inspect the activities of NPOs and separate subdivisions, if necessary, with the involvement of experts (cl. 47 and 48 of the Regulation on the procedure of state registration of NPOs of 10.03.2014 No. 57 approved by the CM).

1413. The Republic of Uzbekistan imposed a wide range of transparency obligations on NPOs (Article 8 of Law of 14.04.1999 No. 763-I) to enable control and supervision over them, and gave sufficient powers to the relevant state bodies authorized to control (monitor) and supervise NPOs, the main role among which is assigned to the MJ.

1414. These state decisions cover most of the measures mentioned as examples in sub-clause 6(b) of the Interpretive Note to Recommendation 8.

1415. In addition to general regulatory and control measures, the legislation also provides specific targeted measures (obligation to publish reports, supervising the collection and expenditure of funds and donations, etc.) concerning vulnerable to TF purposes NPOs. Specific control measures are based on the RBA and are applied together with the general ones within a unified regulatory and control mechanism. Sanctions are foreseen for non-compliance with specific measures.

1416. Applying these measures together permits coping with the existing risk of NPOs being used for TF purposes.

Criterion 8.4

a) As already indicated in Criterion 8.3, the Republic of Uzbekistan has given sufficient powers to the relevant state bodies authorized to control (monitor) and supervise NPOs, including the compliance of NPOs with the requirements of Recommendation 8. All NPOs are subject to state registration. According to Article 8 of Law of 14.04.1999 No. 763-I, non-state NPOs are obliged to provide access to information on the use of their property and funds, including the sources of funding; submit reports on their activities to the registration authority, state tax authorities and state statistics authorities in accordance with the established procedure. There are obligations for beneficiaries to keep records of charitable donations received, to disclose information about charitable donations received within ten days of their receipt in mass media, and if available - on their official websites (Article 51 of Law of 02.05.2007 No. ZRU-96). Public foundations are obliged to publish annual reports on their activities and conduct annual audits of their activities in accordance with the law (Articles 25 and 33 of Law of 29.08.2003 No. 527-II).

b) A wide range of sanctions can be applied for violations of the NPO legislation, which are proportionate and dissuasive. With regard to NPOs or persons acting on their behalf, the Ministry of Justice has the right to (i) make binding submissions to eliminate identified violations of the legislation, founding documents in the activities of NPOs; and (ii) to issue written warnings to officials on the inadmissibility of violations of the law. The Code of Administrative Offences (CAO) provides for administrative responsibility of individuals for "Violation of the order of carrying out activities by non-state non-profit organizations" (Article 239) and "Exceeding the established limits of expenses by a public foundation and failure to publish an annual report" (Article 239^1). Sanctions of these Articles provide for a fine of fifteen to thirty RSV, for officials - thirty to fifty RSV, or administrative arrest for up to fifteen days. In case the public fund exceeds the established expenditure limits, Article 239^1 of the CAO also provides for confiscation of funds in the amount exceeding the expenditure limit. Administrative liability of NPOs as is not envisaged. The bodies of justice (the MJ and its subdivisions) and prosecutor's offices have the right to submit a proposal to the court to suspend the activities of an NPO for up to six months in connection with its violation of the law, as well as for committing acts contrary to its statutory purposes. According to Article 53 of the Civil Code, a legal entity (including NPOs) can be liquidated by a court decision in case of carrying out activities without a permit (license) or activities prohibited by law, as well as in other cases stipulated by the Civil Code. Provisions on forced liquidation of NPO and the mechanism of its implementation are contained in the Regulation on the Procedure of liquidation of NPOs of 15.01.2015 No. 5 approved by the CM of the Republic of Uzbekistan. Individuals are subject to criminal liability for illegal organization of public associations or religious organizations (Article 216 of the CC). Such an act is punishable by a fine of fifty to one hundred RSV (reference calculation value) or restriction of freedom for two to five years, or imprisonment for up to five years. Criminal liability is also provided for inducing participation in the activities of illegal public associations and religious

organizations (Article 216^1 of the CC) and violation of the legislation on religious organizations (Article 216^2 of the CC). The criminal liability of NPOs, as well as others, is not stipulated by the legislation due to the fundamental principles of the legal system. Besides that, the FIU has the authority in cases stipulated by the legislation to apply the procedures and mechanism of suspension of transactions, freezing of monetary funds or other assets of NPOs suspected of TF or other forms of terrorist activity (General Prosecutor's Order of 30.09.2016 No. 22-B). The application of sanctions against NPOs does not prevent civil, administrative or criminal proceedings against the persons acting on behalf of NPOs.

Criterion 8.5

a) The Republic of Uzbekistan has created conditions for effective cooperation, coordination and information-sharing to the maximum extent possible between all levels of the relevant authorities or organizations that have material information on NPOs. Mechanisms of interaction between the relevant authorities are contained in the Regulation on the procedure of interaction between justice authorities and other state administration bodies, local public authorities, LEAs to identify NPOs that violate the law, approved by the resolutions of the CM of 23.10.2018 No. 854 and 09.10.2019 No. 858 "On approval of the regulation on the procedure for approval with the registration authority of receipt by NPOs of monetary funds and assets from foreign States, international and foreign organizations, citizens of foreign States or on their behalf from other persons". Besides that, information may also be obtained from publicly available information resources of state bodies. The register of NPOs can be found on the website of the Ministry of Justice at https://www.minjust.uz. Information about, including NPOs (founders, activities, address, head, etc.) is available on the website of the State Statistics Committee at http://registr.stat.uz.

b) The Republic of Uzbekistan has the capacity to investigate those NPOs suspected of being used in terrorist activities or by terrorist organizations or actively supporting them. Under Article 9 of the AML/CFT Law, the DCEC (FIU) together with LEAs and other state bodies, determines the procedure of interaction for the exchange and transfer of information and data related to AML/CFT/CPF. Information on such joint documents with the MIA, STC and SCC is provided, but they are marked as restricted. The LEAs has the ability to use a range of investigative techniques to conduct TF investigations, including those involving NPOs. See Recommendation 31 for more details on the LEAs' authority.

c) The Republic of Uzbekistan has ensured the possibility of access by the competent authorities to information on the administration and management of a particular NPO (including financial and program information) during the relevant investigation or inspection. Such possibility for the MMJ is provided in the Regulation on the procedure for monitoring and studying the activities of NPOs by justice bodies approved by Resolution of the CM of 08.08.2018 No. 635. The Justice Ministry has the right to receive information about NPOs that constitute a banking secrecy, if this information is necessary for the implementation of its assigned tasks in the field of monitoring compliance with the law in their activities (Article 8 of the Law of the Republic of Uzbekistan of 30.08.2003 No.530-II "On Banking Secrecy"). The DCEC, in accordance with Article 9 of the AML/CFT Law, requests and receives, free of charge, information necessary for the implementation of AML/CFT/CPF measures, including from automated information and reference systems and databases. The FIU is also an OIA and an investigative body, and, therefore, is empowered by the relevant regulations to obtain access to information on the administration and management of a particular NPO (see Recommendation 31). The competent LEAs and investigative bodies obtain information on accounts and deposits held or controlled by individuals or legal persons, including NPOs, and persons acting on behalf of NPOs.

d) The above legislative mechanisms for ensuring cooperation between government authorities provide for their use for rapid transfer to the appropriate competent authorities for taking preventive or investigative measures in cases of suspicion or if there are reasonable grounds to suspect that a particular NPO: (i) is used for TF purposes and/or is a front for fundraising by a terrorist organization; (ii) is used as a channel for TF, including to avoid freezing funds or other forms of support for terrorists; (iii) conceals or obscures the clandestine diversion of funds intended for legitimate purposes, but diverted to the benefit of terrorists or terrorist organizations.

Criterion 8.6

1417. The Ministry of Justice is authorized to respond to international requests on NPOs, and has the ability to maintain, within its authority, direct communication with the bodies of foreign states and international organizations (cl. 12 of the Regulation on the Ministry of Justice approved by Presidential Decree of 13.04.2018 No. PP-3666).

1418. Besides that, the FIU has the authority to consider international requests for information, on specific NPOs suspected of TF or other forms of terrorist activity, within the procedure and mechanism of suspension of operations, freezing of monetary funds or other assets (Chapter 6 of the Regulation in the General Prosecutor's Order of 30.09.2016 No. 22-B).

Weighting and Conclusion

1419. Comprehensive information from relevant sources was not used to determine the types of NPOs at risk of TF and the level of risk. The list of such sources was unnecessarily limited.

1420. The NRA and SRA did not consider the threat posed to NPOs by terrorist entities.

1421. There was insufficient engagement with NPOs to develop and improve methods to identify and mitigate the risk of TF and related vulnerabilities.

1422. There is a lack of information on implementing special programmes to encourage NPOs to conduct transactions through regulated financial channels.

1423. Administrative liability of NPOs as legal entities is not legislated.

1424. **Recommendation 8 is rated Partially Compliant.**

Recommendation 9 - Financial institution secrecy laws

1425. In the 2010 mutual evaluation report, the Republic of Uzbekistan was rated under R.4 as "PC". The main deficiencies were related to unclear powers of supervisory authorities (except for the Central Bank) in terms of regulations on commercial secrecy.

Criterion 9.1

1426. Availability of information to competent authorities. The legislation stipulates that providing information on transactions in monetary funds or other assets of and individuals or other information to a specially authorized state body (the DCEC) in accordance with the established procedure is not a violation of commercial, banking or other secrets protected by law (Article 18 of the AML/CFT Law). Similar obligations for FIs can be found in the specific legislation (Articles 5, 8 of Law of 30.08.2003 No. 530-II, Article 5 of Law of 11.09.2014 No. ZRU-37, Article 26 of Law of 05.04.2002 No. 358-II, Article 51 of Law of 22.07.2008 No. ZRU-163, Article 16 of Law of 12.09.2014 No. ZRU-375), and in the ICR for postal service operators (ICR of 28.08.2018 No. 3061). There are no special requirements for leasing companies and pawnshops, except for general requirements in the AML/CFT Law, however, this does not have a significant impact on the overall assessment.

1427. The legislation provides for the right of LEAs, which carry out criminal intelligence and detective operations, to receive such information directly from FIs. In accordance with Article 9 of Law of 30.08.2003 No. 530-II, the LEAs of the Republic of Uzbekistan can receive information about the existence of bank accounts for the purposes of criminal intelligence gathering and for criminal cases, which are being investigated (see R.31.1a, 31.3a).

1428. In terms of the exchange of information between competent authorities at national and international level, there are no obstacles from the law on the protection of financial institution secrecy. The Republic of Uzbekistan has presented a number of regulations on cooperation between the DCEC and some LEAs (see R.31.4.). These documents regulate the exchange of information between competent authorities, including information containing bank secrecy. The exchange of information between competent authorities at the international level is regulated by the Regulation on the Procedure of International Cooperation in the Field of AML/CFT/CPF, approved by the Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 402 of 29.06.2021.

1429. There are a number of legal restrictions for FIs to exchange information required for the purposes of:

- R.13: banks and microcredit organizations can exchange and provide each other information about their customers only for the purpose of ensuring the safety of their activities, deposit insurance, loan repayment and other investments in the manner and within the limits prescribed by law (Art. 14 of Law of 30.08.2003 No. 530-II "On Bank Secrecy", Art. 16-1 of Law of 20.09.2006 No. ZRU-53).
- R.16: the above restriction applies to the exchange of information between banks for the purpose of transferring information on the originator and beneficiary of transfers, as it is more enforceable than the rules set out in the ICR. Payment system operators and payment service providers are also obliged to ensure confidentiality of information obtained by them in the course of providing payment services, do not allow its disclosure to third parties, except as provided for in the Law on Bank Secrecy (Article 17 of Law of 01.11.2019 No. ZRU-578). For postal money transfers R.9 is met, as Article 16 of Law of 22.04.2009 No. ZRU-211 provides an exception to the rule on secrecy of postal transfers for cases established by law, which includes ICR.
- R.17: the above restrictions also apply to cases of disclosure to third parties under R.17. In addition, disclosure of confidential information in the securities market is carried out in the cases and manner provided for by Law of 03.06.2015 No. ZRU-387 (Article 50), which does not provide for the exchange of such information between FIs. For insurance companies, the criterion norms are met as, in accordance with Article 26 of Law No. 358-II of 05.04.2002 "On Insurance Activities", confidential information may be disclosed to third parties (including FIs) based on the written consent of the insured and insured persons and beneficiaries in relation to information concerning them.

Weighting and Conclusion

1430. There are a number of legal restrictions for FIs to exchange information.

1431. **Recommendation 9 is rated Largely Compliant.**

Recommendation 10 - Customer due diligence (CDD)

1432. In the MER 2010, the Republic of Uzbekistan was rated under R.5 as "PC". This rating was due to the following factors: the established threshold for conducting CDD on one-time transactions did not meet the requirements of the Standards, verification of the beneficial owner identity was not carried out on the basis of reliable sources, , there was no requirement to carry out enhanced CDD in relation to high-risk customers, transactions and business relationships,. After the adoption of the AML/CFT Law, an assessment of the existence of anonymous accounts was not carried out and there was no requirement to close them if there were indicators of anonymity. The AML/CFT system of the Republic of Uzbekistan did not contain special requirements and mechanisms for their implementation for applying CDD measures in relation to existing customers.

Criterion 10.1

1433. FIs must refuse to cooperate with customers who have not provided the documents required for identification, except for operations on crediting funds to an account (Article 16 of the AML/CFT Law). This exemption does not affect the rating as the customer who opened the account is identified. Similar obligations are also set in the ICR for the securities sector (cl. 18 of the ICR No. 2033 of 03.11.2009), exchange members (cl. 24 of the ICR No. 2038 of 06.11.2009), leasing companies (cl. 19 of the ICR No. 2011), insurance sector when establishing a business relationship (cl. 16 of the ICR No. 2036 of 03.11.2009). In addition, all credit institutions are prohibited from opening or maintaining anonymous accounts or accounts under fictitious names (paragraph 45 of ICR No. 2886 of 23.05.2017, cl. 33 of ICR No. 2925 of 04.09.2017). Payment institutions are prohibited from conducting money transfers before clients' CDD (cl. 30 of the ICR No. 3266 of 30.06.2020). There is no information on a similar prohibition for custody accounts of professional participants in the securities market. Operators of e-money systems do not conduct CDD of the e-money holder when the maximum amount of one transaction performed by an individual does not exceed the amount

equal to the size of the base settlement unit; when the maximum amount of e-money stored in one electronic device does not exceed the amount of 5 times the size of the base settlement unit (cl. 17 of ICR No. 3266 of 30.06.2020). Thus, the legislation allows for the maintenance of anonymous (unidentified) e-wallets for very limited amounts (USD 113).

Criterion 10.2

1434. FIs are obliged to apply CDD measures:

a) when establishing a business relationship (Article 7 of the AML/CFT Law);

b) Banks - when conducting one-time transactions, including by performing one or related transactions, for an amount exceeding 100 RSV (2500 USD)[125], 300 RSV (7500 USD) or 500 RSV (11000 USD), depending on the type of transaction, i.e. for major occasional transactions, but not for all, without exception (cl. 22 of the ICR of 23.05.2017 No. 2886);

   NBCIs - for a one-time provision of services in an amount exceeding 10 RSV (250 USD) (cl. 21b of the ICR of 04.09.2017 No. 2925);

   insurance companies - when carrying out one-time transactions, the amount of which exceeds 300 RSV (7500 USD) on the day of the operation (cl. 16 of the ICR of 03.11.2009 No. 2036) ;

   postal operators - when providing services for making and delivery of transfers (cl. 18 of the ICR of 28.08.2018 No. 3061);

   professional participants in the securities market – when conducting transactions the amount of which exceeds 500 RSV (12500 USD) (cl. 12 of the ICR of 03.11.2009 No. 2033);

   exchange members - when conducting transactions, the amount of which exceeds 500 RSV (12 500 USD) (cl. 16 of the ICR of 06.11.2009 No. 2038);

   leasing companies - when conducting one-time transactions, the amount of which exceeds 300 RSV (7500 USD) on the day of the operation (cl. 13 of the ICR of 22.09.2011 No. 2265);

   sector of payment organisations does not conduct CDD when the maximum amount of electronic money stored in one electronic device of a person who is the owner of electronic money does not exceed 5 RSV (125 USD) (cl. 17 of the CCP of 30.06.2020 №3266);

c) when conducting transfers, as required by R.16, except for certain transactions between individuals, payments for utilities, communication services, payments to the budget, off-budget funds and other obligatory payments, electronic money transfers (cl. 22, 38 of the ICR of 23.05.2017 No. 2886; cl. 18 of the ICR of 28.08.2018 No. 3061, cl. 17 of the ICR of 30.06.2020 No. 3266). That is, there are limited cases of legal exemptions where CDD of the client is not carried out (see R.16.1));

d) when conducting transactions that arouse suspicion of ML/TF (Article 7 of the AML/CFT Law);

e) if there are doubts about the reliability of previously obtained data on the identity of the customer (Article 7 of the AML/CFT Law).

Criterion 10.3

1435. As a CDD measure, FIs verify the identity and authority of the customer (both permanent and occasional) and the persons on whose behalf he acts on the basis of the relevant documents, and also identify the owner or the person controlling the customer (if the customer is a legal entity) by studying the ownership and management structure on the basis of constituent documents (Article 7 of the AML/CFT Law).

1436. The obligation to verify customer data is established in the basic law (Article 15 of the AML/CFT Law) and in sectoral ICRs. Verification of documents of individuals is provided through an appeal to the information system of the MIA (Article 26 of the ICR of 23.05.2017 No. 2886, Article 26 of the

[125] The reference calculation value is equal to 270000 soums (clause 7 of Presidential Decree of 30.12.2019 No. PP-4555) or 25 USD at the rate of 01.09.2021.

ICR of 04.09.2017 No. 2925), - through an appeal to the automated state registration system (Article 26 of the ICR of 23.05.2017 No. 2886). Furthermore, FIs in relation to legal entities shall use information from publicly available state sources, e.g. automated state registration system (banks – cl. 25-27, 30 Annex 1, 2 of the ICR No. 2886 of 23.05.2017; NBCI – cl. 24-26, Annex 1, 2 of the ICR No. 2925 of 04.09.2017; payment organizations – cl. 26, 28 of the ICR No. 3266 of 30.06.2020; postal operators – cl. 26 of the ICR No. 3061 of 28.08.2018; professional securities market participants – cl. 14, ICR No. 2033 of 03.11.2009; stock exchange members - cl.19, 20, 22 ICR No. 2038 of 06.11.2009; leasing companies - cl.15, 17, ICR of 22.09.2011 No. 2265). When state databases are insufficient, FIs are obliged to verify client information from other publicly available sources of information, information from other organisations.

1437. The legislation does not provide for specific features in the mechanism of identification of legal arrangements. For a number of FIs an analogy of their identification and verification with legal entities is established: from 25.12.2020 for banks (cl. 1, 291 of ICR No. 2886), NBCI (cl. 1, 281 of ICR No. 2925), from 14.06.2021 for exchange members (cl. 1, 40 of ICR No. 2038) from 17.06.2021 for leasing companies (cl. 29 of ICR No. 2265).

1438. For the insurance sector, there are no requirements to conduct detailed CDD on the basis of identity documents, registration and other documents to verify the identity of the customer. For the securities sector there is a limited list of sources (public authorities and other organisations) to verify the information provided by the customer, but this is recognised by assessors as sufficient for the sector.

Criterion 10.4

1439. The requirements to verify the identity and authority of the customer, its representatives and persons on whose behalf the customer acts on the basis of relevant documents are implemented in the Internal Control Rules (icr) and other specialized legislation for financial institutions: for banks (cl. 23 of the ICR of 23.05.2017 No. 2886, cl. 12-14, 16, 17 of the Instructions on bank accounts of 27.04.2019 No. 1948), NBCIs (cl. 22 of the ICR of 04.09.2017 No. 2925), sector payment organizations (cl.17 of the ICR of 30.06.2020 No. 3266), insurance companies (cl. 21 of the ICR of 03.11.2009 No. 2036), postal operators (cl. 136-138 of the Rules for the provision of postal services of 18.04.2011 No. 2219) and exchange members (cl. 16^2 of the ICR of 06.11.2009 No. 2038), professional participants in the securities market (cl. 13-2 of ICR No. 2033 dd. 03.11.2009) and leasing companies (cl. 13-3 of ICR No. 2265 dd. 22.09.2011)..

Criterion 10.5

1440. The definition of a BO (beneficial owner) is contained in the ICR for FIs[126] and is consistent with the definition in the FATF Glossary. FIs are obliged to identify and verify BO during CDD (such a duty is included in the Art. 7 and 15 of the AML/CFT Law as well as in the all ICRs for FIs). The basis for BO identification is constituent documents (Article 7 of the AML/CFT Law). No other documents have been established for these purposes.

Criterion 10.6

1441. As part of CDD measures, FIs are obliged to constantly study the business relationships and transactions carried out by the customer in order to verify their compliance with the information about such a customer and his activities (Article 7 of the AML/CFT Law). The obligation to study the purpose and nature of business relations is enshrined in the ICR for banks, NBCIs, payment organizations, postal operators, leasing companies and professional participants in the securities market (cl. 23 of the ICR of 23.05.2017 No. 2886, cl. 22 of the ICR of 04.09.2017 No. 2925, cl. 17 of the ICR of 30.06.2020 No. 3266, cl. 22 of the ICR of 28.08.2018 No. 3061, cl. 10 of the ICR of 22.09.2011 No. 2265), cl. 13-2 of ICR No. 2033 of 03.11.2009). Insurance companies and exchange members are obliged to determine the type of operation and the extent of its compliance with the

[126] The natural person who ultimately owns or actually controls a customer, including the legal entity for whose benefit the transaction in monetary funds or other assets is being conducted.

purpose of the customer's activity (and the type of activity, if the customer is an individual) (cl. 19 of the ICR of 03.11.2009 No. 2036, cl. 18 of the ICR of 06.11.2009 No. 2038). Therefore, FIs are obliged to understand that the purpose and intended nature of the business relationship with the client is in line with the client's business profile.

Criterion 10.7

a) The requirement to conduct continuous monitoring of transactions for their compliance with the customer's business, its level of risk and source of income is enshrined in the Internal Control Rules for banks and NBCIs, payment organizations and postal operators (cl. 23, 48, 63 of the ICR of 23.05.2017 No. 2886; cl. 22, 43 of the ICR of 04.09.2017 No. 2925, cl. 17, 23 of the ICR of 30.06.2020 No. 3266, cl. 19, 41 of the ICR of 28.08.2018 No. 3061). There is no legal requirement for leasing companies, insurance companies, professional participants in the securities market and exchange members to conduct an analysis of compliance of transactions with the level of risk of working with a customer.

b) The requirements to keep transaction information, identification data and CDD material, and to update it periodically, including at least annually in cases of high ML/TF risk by the customer, are set in the Internal Control Rules for banks (cl. 89, 94, 95 of the ICR of 23.05.2017 No. 2886), NBCIs (cl. 27, 30, 70 of the ICR of 04.09.2017 No. 2925), payment organizations (clauses 55, 58 of the ICR of 30.06.2020 No. 3266), exchange members (cl. 16, 23, 27, 37 of the ICR of 06.11.2009 No. 2038); insurance companies (cl. 30-6, 32 of ICR Nos. 2036 of 03.11.2009), and professional participants in the securities market (cl. 27-3 of ICR No. 2033 of 03.11.2009), postal operators (cl. 63, 66 of the ICR of 28.08.2018 No. 3061), leasing companies (cl. 131 , 17 of the ICR of 22.09.2011 No. 2265). However, ICR for insurance companies do not have the specific requirement to update information, obtained as a result of CDC measures for high-risk customers.

Criterion 10.8

1442. Banks, NBCIs, exchange members, payment organizations sector, leasing companies, insurance companies, professional participants in the securities market, postal operators are required to study the ownership and management structure of customers who are legal entity (cl. 27, 29 of the ICR of 23.05.2017 No. 2886, cl. 27, 28 of the ICR of 04.09.2017 No. 2925, cl. 21 of the ICR of 06.11.2009 No. 2038, cl.28 of the ICR of 30.06.2020 No. 3266,cl. 16 of the ICR of 22.09.2011 No. 2265, cl. 21-1 of ICR No. 2036of 03.11.2009, cl. 16-1 of ICR No. 2033 of 03.11.2009, cl. 27 of ICR No. 3061 of 28.08.2018). The legislation uses the term 'study' instead of 'understanding', which does not quite meet the criterion requirement.

1443. There are no rules for postal operators, professional securities market participants and insurance companies on the study of the nature of the activity, ownership structure and management of customers who are legal arrangements.

1444. The customer due diligence measures taken by banks necessarily include the study of the purpose and nature of the business relationship or planned operations (cl. 23 of the ICR of 23.05.2017 No. 2886).

1445. Similar amendments were made for NBCIs and for payment organizations sector (cl. 1, 281, 22 of the ICR of 09.12.2020 No. 2925, cl.17 of the ICR 3266 of 30.06.2020). There are no obligations for other FIs to understand the nature of the business of customer who is a legal person or a legal arrangement.

Criterion 10.9

a) Banks, NBCIs, postal operators , leasing companies and exchange members are required to identify and verify the data of a customer who is a legal entity based on information and its name (which contains an indication of the legal form), state registration, individual taxpayer number, existing licenses and other information confirming its existence (cl. 25 of the ICR of 23.05.2017 No. 2886, cl. 24 of the ICR of 04.09.2017 No. 2925, cl. 24, 26 of the ICR of 30.06.2020 No. 3266, cl. 24 of the ICR of 28.08.2018 No. 3061, cl. 15 of the ICR of 22.09.2011 No. 2265, cl. 17 and Annex 2 of the ICR No.

2038 of 06.11.2009); there is no detailed list of customer data for identification in the ICR for insurance companies, professional participants in the securities market;

b) Banks, NBCIs, postal operators, payment organizations sector, exchange members are required to examine the powers of the legal entity, as well as the names of specific individuals occupying senior positions in the legal entity (cl. 27 of the ICR of 23.05.2017 No. 2886, cl. 27 of the ICR of 04.09.2017 No. 2925, cl. 26 of the ICR of 28.08.2018 No. 3061, cl. 24, 26 of the ICR of 30.06.2020 No. 3266, cl.17 of the ICR of 06.11.2009 No. 2038); the ICR for insurance companies, professional securities market participants and leasing companies have no detailed customer data list for identification;

c) All the ICR for financial institutions, except for ICR for insurance companies, stipulates the obligation to receive information on the location (address) of a legal entity during CDD; insurance companies must receive the relevant documents on state registration, as well as the information specified in the constituent documents (cl. 21 of the ICR of 03.11.2009 No. 2036).

Criterion 10.10

1446. FIs are obliged to identify owners and persons controlling customers, as well as take available measures to verify their identity (Article 15 of the AML/CFT Law.

a) FIs are obliged to identify owners and persons controlling customers, as well as take available measures to verify their identity (Article 15 of the AML/CFT Law). There is no concept of a "beneficial owner" in the AML/CFT law. The notion of beneficial ownership in the ICR[127] does not explicitly include a controlling interest, with the exception of the ICR for the payment institution sector, where the controlling interest in the ultimate legal entity or entity without legal personality (if any) is set at a level not less than ten percent (cl. 27 of the ICR of 30.06.2020 No. 3266, cl. 27 of the ICR No. 2886 of 23.05.2017).

b) Banks are obliged to identify an individual who is the beneficial owner of the customer and who ultimately owns or controls the customer (cl. 27 of the ICR of 23.05.2017 No. 2886) NBCIs (cl. 34 of the ICR of 04.09.2017 No. 2925), exchange members (cl. 1, 16-2 of the ICR of 06.11.2009 No. 2038), payment organizations sector (cl. 17, 27 of the ICR of 30.06.2020 No. 3266), postal operators (cl. 27 of the ICR of 28.08.2018 No. 3061), leasing companies (cl. 13-3 of the ICR of 22.09.2011 No. 2265), insurance companies (cl. 15-1 of the ICR of 03.11.2009 No. 2036),professional participants of the securities market (cl. 13-2 of the ICR of 03.11.2009 No. 2033).

c) For banks, NBCIs, exchange members, payment organizations sector, postal operators, leasing companies, insurance companies and professional participants of the securities market the obligation of the financial institution has been established to recognize the head of a legal person as the beneficial owner (cl. 27 of the ICR of 23.05.2017 No. 2886, cl. 27 of the ICR of 04.09.2017 No. 2925), cl. 16-2 of ICR of 06.11.2009 No. 2038, cl. 28 of the ICR of 30.06.2020 No. 3266, cl. 27 of ICR of 28.08.2018 No. 3061, cl. 13-3 of ICR No. 2265 of 22.09.2011 No. 2265, cl. 16-1 of the ICR of 03.11.2009 No. 2036 with amendments of 26.06.2021).

Criterion 10.11

1447. Creation of legal arrangements (trusts and other arrangements) in the Republic of Uzbekistan is not provided ("Decree of the Cabinet of Ministers of the Republic of Uzbekistan of 09.02.2017 No. 66 "On measures to implement the Decree of the President of the Republic of Uzbekistan of 28 October 2016 No. PP-2646 "On improvement of the state registration and registration system of business entities"). Foreign trusts and other forms of collective investment and (or) trust management are subject to the requirements of the legislation of Uzbekistan (Article 35 of the Tax Code of the Republic of Uzbekistan). Postal operators, professional securities market participants and insurance companies are not obliged to conduct CDD in relation to foreign trusts and other forms of collective investment and/or trust management. The obligation to identify the person exercising ultimate control

[127] The natural person who ultimately owns or has effective control over a customer, including the legal person for whose benefit a transaction involving money or other property is being conducted.

over a trust and other legal arrangement is established for banks, NBCIs, exchange members, payment organizations sector and leasing companies by analogy as for a legal entity (without regard to any specifics) (cl. 29-1 of the ICR of 23.05.2017 No. 28886, cl. 28-1 of the ICR of 04.09.2017 No.2925, cl. 40 of the ICR of 06.11.2009 No.2038, cl. 26,27 of the ICR of 30.06.2020 No.3266, cl. 13-3 of the ICR of 22.09.2011 No. 2265) and hence, all references to the ICR duplicating criterion 10.10.

Criterion 10.12.

a) to ascertain the name of the beneficiaries of life insurance policies, the presentation of the document proving the identity of the beneficiary is required in limited cases, namely, only in case of death of the insured person in connection with the performance of his functional duties (applies only to judges and employees of rescue teams);

b) measures to identify the beneficial owner or beneficiary must be taken before making payments under insurance contracts (cl. 18 of the ICR of 03.11.2009 No. 2036), no requirement for classes of beneficiaries;

c) there is no information on the obligation to verify the identity of the beneficiary at the time of the insurance payment.

Criterion 10.13

1448. Insurance companies are not required to consider receiving a life insurance premium as an important risk factor when deciding whether to apply EDD measures. A general requirement was established to take measures to determine, assess and mitigate the level of risk of customers conducting transactions for ML/TF purposes (Article 23^1 of the ICR of 03.11.2009 No. 2036).

Criterion 10.14

1449. FIs are required to apply CDD measures when establishing business relationships or performing transactions for one-time customers (Article 7 of the AML/CFT Law). Delayed identification is not provided for in the legislation.

Criterion 10.15

1450. Entry into a business relationship is not foreseen before the identity is verified (see Criterion 10.14).

Criterion 10.16

1451. Banks, NBCIs,postal operators, exchange members, payment institutions sector are obliged to apply CDD measures to existing customers by updating previously received information (i.e. identification data, purpose and nature of business activities, financial situation and business reputation of customers, origin of funds and property of customers) depending on their risk profiles and data previously established (cl. 42, 94 of the ICR of 23.05.2017 No. 2886; cl. 30.70 of the ICR of 04.09.2017 No. 2925; cl. 17 of the ICR of 28.08.2018 No. 3061; cl.17, 23 ICR of 06.11.2009 № 2038, cl. 29 ICR of 30.06.2020 №3266). Specific update depending on the level of risk have been set for banks and NBCIs, operators, postal service providers, exchange members, payment institutions sector.

1452. Insurance companies carry out a one-time update of information about existing customers at the time of the entry into force of the ICR (cl. 16 of the ICR of 03.11.2009 No. 2036). Professional participants in the securities market are not required to take into consideration ML/TF risks. The relevant requirements for leasing companies have not been established.

Criterion 10.17

1453. FIs are obliged to apply enhanced CDD measures in relation to higher-risk customers, including if one of the parties to the transaction is a person residing, staying or registered in a state that does not participate in international AML/CFT cooperation or in an offshore zone (banks - cl. 57 of the ICR of 23.05.2017 No. 2886; NBCIs - cl. 45 of the ICR of 04.09.2017 No. 2925; sector of payment organisations – cl. 23, 34 of the ICR No. 3266 of 30.06.2020, insurance companies - cl. 16^2 of the ICR of 03.11.2009 No. 2036; professional participants in the securities market - cl. 13 of the ICR of

03.11.2009 No. 2033; leasing companies - cl. 13^1 of the ICR of 22.09.2011 No. 2265) or when the operation is categorized higher risk (postal operators - cl. 36 of the ICR of 28.08.2018 No. 3061) or when a higher level of risk is established (exchange members - cl. 27 of the ICR of 06.11.2009 No. 2038).

Criterion 10.18

1454. There is a declarative provision on the possibility of applying measures of controls according to the risks identified (Article 7^1 of the AML/CFT Law). Nevertheless, the ICR for FIs does not allow of applying simplified CDD measures.

Criterion 10.19

1455. FIs are obliged, if it is impossible to apply CDD measures, refuse to open an account, conduct a transaction, enter into a business relationship and terminate an existing relationship, as well as file a STR to the DCEC (Article 15 of the AML/CFT Law).

Criterion 10.20

1456. The legislation does not provide for permission for FIs (excluding exchange members, sector of payment organisations and operators, postal service providers) not to carry out CDD if there is suspicion of ML/TF, but to file STRs instead.

Weighting and Conclusion

1457. The Republic of Uzbekistan has mostly implemented the CDD requirements. FIs are obliged to identify customers who are natural persons on the basis of original identity documents or biometric data, and legal persons - on the basis of constituent documents; verification shall be conducted using state databases. FIs are required to establish beneficial owners of both natural and legal persons.

1458. At the same time, there are few deficiencies: for banks and NBCIs the obligation to carry out CDD on threshold amounts is established not for all one-off transactions, but for their closed list; there are very limited statutory exemptions where no customer CDD is carried out when making a transfer; the legislation uses the term 'study' instead of 'understanding' of the client's ownership and management structure, which does not quite meet the requirement of the standards; there are deficiencies in the insurance sector related to confirming the identity of the recipient of the insurance benefit; The AML/CFT Law does not oblige financial institutions to carry out CDD of foreign structures without forming a legal entity considering their specificities; there is no legal provision for FIs (other than members of exchanges, payment organizations sector and operators, postal service providers) not to conduct CDD where there is suspicion of ML/TF, but instead to send an STR.

1459. **Recommendation 10 is rated Largely Compliant.**

Recommendation 11 - Record keeping

1460. In the 2010 mutual evaluation report, the Republic of Uzbekistan was rated under R.10 as "LC" due to the absence of requirements for storing records in a format that provides timely access of competent authorities.

Criterion 11.1

1461. FIs are obliged to keep records on all transactions in monetary funds or other assets for at least five years after conducting such transactions or termination of business relations with customers (Article 21 of the AML/CFT Law, banks - cl. 89 of the ICR of 23.05.2017 No. 2886, NBCIs - cl. 66 of the ICR of 04.09.2017 No. 2925, professional participants in the securities market - cl. 26 of the ICR of 03.11.2009 No. 2033, exchange members - cl. 37 of the ICR of 06.11.2009 No. 2038, insurance companies - cl. 32 of the ICR of 03.11.2009 No. 2036, leasing companies - cl. 27 of the ICR of 22.10.2011 No.2265, postal operators - cl. 63 of the ICR of 28.08.2018 No. 3061). This requirement applies to both domestic and international transactions.

Criterion 11.2

1462. FIs are required to keep identification data and CDD data for at least five years after the termination of business relationships with customers (Article 21 of the AML/CFT Law). These requirements, including the requirement for keeping business correspondence, are also enshrined in the ICR for FIs in the provisions related to the implementation of Criterion 11.1 (see above). The requirement to keep the results of any analysis undertaken is stipulated by the ICR for banks No. 2886-6 as amended on 25.12.2020 and ICR for NBCIs No. 2925-4 as amended on 09.12.2020, the ICR for members of exchanges as of 14.06.2021 No. 2038-5, the ICR for payment organisations as of 24.06.2020 No. 3266 (item 55), and the ICR for postal operators as of 26.06.2021 No. 3061-2 whereas ICR of leasing and insurance companies do not contain the requirements mentioned above.

Criterion 11.3

1463. The requirements that transaction records must be sufficient to permit the reconstruction of individual transactions in order to serve as evidence in the prosecution of criminal activity, if necessary can be found in the ICR for financial institutions (banks - cl. 88 of the ICR of 23.05.2017 No. 2889; NBCIs - cl. 65 of the ICR of 04.09.2017 No. 2925, professional participants in the securities market - cl. 26 of the ICR of 03.11.2009 No. 2033, exchange members - cl. 131 of the ICR of 06.11.2009 No. 2038, insurance companies - cl. 30-5 of the ICR of 03.11.2009 No. 2036, leasing companies - cl. 11 of the ICR of 22.10.2011 No. 2265, postal operators - cl. 65 of the ICR of 28.08.2018 No. 3061, payment institution sector – cl. 54-55 of ICR of 30.06.2020 No. 3266).

Criterion 11.4

1464. LEAs have the right to send inquiries to organizations (Article 36 of the CPC), and managers and other officials of enterprises, institutions, organizations are obliged, at the request of an inquirer, investigator, prosecutor or court, to submit documents in their possession or specially prepared on the basis of the information they have (Article 201 of the CPC). In accordance with the ICR for FIs, information on operations should be drawn up in such a way that, if necessary, it would be possible to restore the details of the operation (see Criterion 11.3). Also, the DCEC has the right to receive information on transactions in monetary funds or other assets (cl. 20-21 of Resolution of the Cabinet of Ministers of 12.10.2000 No. 272, cl. 6 of Presidential Decree of 23.05.2018 No. 5446).

Weighting and Conclusion

1465. The legislation contains a requirement to keep records for at least five years from the date of termination of customer service/transaction. However, for leasing and insurance companies, there are no provisions for storing the results of any analysis undertaken, with the exception of data obtained during CDD procedures.

1466. **Recommendation 11 is rated Largely Compliant.**

Recommendation 12 - Politically exposed persons

1467. In the 2010 mutual evaluation report, the Republic of Uzbekistan was rated under R.6 as "NC", as there were no legislative or other measures in accordance with this Recommendation.

1468. The definition of PEP is contained in the Internal Control Rules for banks, NBCIs, professional participants in the securities market, exchange members, and postal operators. This definition includes PEPs from foreign States and international organizations and does not include national PEPs. This definition does not cover persons in military positions as well as former PEPs. There is no definition of PEP for insurance and leasing companies.

Criterion 12.1

a) The requirements have a risk management system in place to determine whether a customer or beneficial owner is a PEP are contained in all ICRs: banks – cl. 23 of ICR No. 2886 of 23.05.2017; NBCI – cl. 4 and 22 of ICR No. 2925 of 04.09.2017; professional securities market participants – cl. 18-2 of ICR dated 03.11.2009 No. 2033; stock exchange members - cl 26 of ICR dated 06.11.2009 No. 2038;

insurance companies – cl. 16-1 of ICR dated 03.11.2009 No. 2036; leasing companies – cl. 19-2 of ICR dated 22.10.2011 No. 2265; postal operators – cl. 20 of ICR dated 28.08.2018 No. 3061; electronic money system operators, payment system operators, and payment organisations – cl. 21 of ICR dated 30.06.2020 No. 3266, auditors – cl.30 of ICR dated 15.12.2018 No. 3101.

b) FIs must establish business relations with PEPs only with the permission of the senior management: banks - cl. 23 of the ICR of 23.05.2017 No. 2886; NBCIs cl. 22 of the ICR of 04.09.2017 No. 2925; professional participants in the securities market cl. 13-3 of the ICR of 03.11.2009 No. 2033; exchange members cl. 16-2 of the ICR of 06.11.2009 No. 2038; insurance companies – cl. 16-1 of ICR dated 03.11.2009 No. 2036; leasing companies – cl. 18-1 of ICR dated 22.10.2011 No. 2265; postal operators - cl. 20 of the ICR of 28.08.2018 No. 3061; electronic money system operators – cl. 21 of ICR dated 30.06.2020 No. 3266.

c) FIs should take reasonable measures to determine the source of funds or other property (wealth) of PEPs under the transactions they carry out, as well as, when applying enhanced CDD measures to PEPs, (banks - cl. 23 of the ICR of 23.05.2017 No. 2886, NBCIs cl. 23 of the ICR of 04.09.2017 No. 2925, professional participants in the securities market - cl. 13-3 of the ICR of 03.11.2009 No. 2033, exchange members cl. 16-2 of the ICR of 06.11.2009 No. 2038, postal operators cl. 20 of the ICR of 28.08.2018 No. 3061, electronic money system operators - cl. 21 of ICR dated 30.06.2020 No. 3266).

d) FIs should conduct ongoing in-depth monitoring of business relations with PEPs (banks - cl. 23 of the ICR of 23.05.2017 No. 2886, NBCIs - cl. 23 of the ICR of 04.09.2017 No. 2925, professional participants in the securities market - cl. 13-3 of the ICR of 03.11.2009 No. 2033, exchange members cl. 16-2 of the ICR of 06.11.2009 No. 2038, insurance companies – cl. 16-1 of ICR dated 03.11.2009 No. 2036 with amendments of 26.06.2021, postal operators - cl. 20 of the ICR of 28.08.2018 No. 3061, electronic money system operators - cl. 21 of ICR dated 30.06.2020 No. 3266).

Criterion 12.2

1469. As already stated above, the definition of PEPs in the ICR for FIs includes PEPs of international organizations, but does not include national PEPs. Thus, all requirements related to PEPs do not apply to national PEPs.

Criterion 12.3

1470. The requirements of this criterion are partially implemented in the ICR of financial institutions (banks - cl. 23 of the ICR of 23.05.2017 No. 2886; NBCIs - cl. 40 of the ICR of 04.09.2017 No. 2925, professional participants in the securities market - cl. 13-3, 18-2 of the ICR of 03.11.2009 No. 2033, exchange members cl. 16-2 of the ICR of 06.11.2009 No. 2038, insurance companies – cl. 16-1 of ICR dated 03.11.2009 No. 2036, postal operators - cl. 20 of the ICR of 28.08.2018 No. 3061, electronic money system operators - cl. 4, 21 of ICR dated 30.06.2020 No. 3266). While the ICR for banks and NBCIs apply certain elements of this criterion to "family members of PEPs or persons closest to PEPs", the ICR for professional participants in the securities market, exchange members and postal operators only deal with close relatives. The compliance with this criterion is influenced by the deficiencies under Criterion 12.2.

Criterion 12.4

1471. Although insurance companies are required to apply measures to PEPs under the requirements of criteria 12.1-12.2 there are no specific risk minimisation requirements in relation to life insurance policies.

Weighting and Conclusion

1472. The legislation of the Republic of Uzbekistan contains certain elements of the requirements for relations with foreign PEPs and PEPs of international organizations. There are significant deficiencies: the definition of PEP in the ICR for FIs does not include national PEPs, military positions and former PEPs of most FIs (except for banks and NBCIs) are not covered; insurance and leasing companies are not assigned any responsibilities related to PEPs.

1473. **Recommendation 12 is rated Partially Compliant.**

Recommendation 13 - Correspondent banking

1474. In the 2010 MER, the Republic of Uzbekistan was rated under R.7 as "PC". The following were noted as the main deficiencies: the lack of a proper elaboration of the mechanism for assessing the respondent bank in terms of AML/CFT issues, the lack of a special procedure for recording this information; the obligation to collect and store information about a correspondent bank was established within the framework of general CDD norms and required details in relation to correspondent banking; the issue of the distribution of responsibilities in the AML/CFT area in the establishment of cross-border correspondent relations was not worked out; lack of regulation of AML/CFT issues in relation to "transit accounts".

Criterion 13.1

a) The requirements the need to collect information on a non-resident bank, an international remittance service provider, in order to get a complete picture of the nature of its business activities; to determine, based on publicly available information, the reputation and quality of supervision, including whether ML/TF violations have been investigated with respect to that bank (company),are established in the ICR (banks - cl. 33 of the ICR of 23.05.2017 No. 2886; postal operators - cl. 23 of the ICR of 28.08.2018 No. 3061).

b) The requirements on the need to ensure that non-resident banks with which correspondent relationships are established apply international AML/CFT standards are established in the ICR for banks - cl. 33, 34 of the ICR of 23.05.2017 No. 2886. For postal operators the corresponding norm of the Postal Payment Services Agreement and its Regulations (Art. RP 707) is applied, which does not explicitly require an assessment of the AML/CFT measures applied by the correspondent institution, but requires to decline to open postal payment services with another designated operator if the latter operator fails to meet its legal obligations to combat money laundering and terrorist financing, which does not fully meet the requirements of this sub-criterion.

c) The board of a bank decides to establish relations with international money transfer systems and correspondent relations with a non-resident bank (cl. 33, 37 of the ICR of 23.05.2017 No. 2886). Postal operators carry out international money transfers on the basis of bilateral Agreements, which are signed by the heads of postal administrations. The duties of the General Director of JSC "Uzbekiston Pochtasi" include making transactions and signing documents on behalf of JSC "Uzbekiston Pochtasi" (Article 129 of the Charter). It is fully compliant with the sub-criterion.

d) According to the amendments made on 25.12.2020 to the ICR No. 2886 when establishing and implementing correspondent relations with a non-resident bank, in addition to identifying a non-resident bank, the bank must ensure a clear and complete distribution of responsibilities between correspondents (cl. 33 of the ICR of 23.05.2017 No. 2886 which meets the sub-criterion. A similar obligation for postal operators is established by Article 4, paragraph 1, of the Universal Postal Union's Agreement on Postal Payment Services, according to which member countries shall take the necessary measures to ensure the continuity of postal payment services in the event of default by their designated operator(s), maintaining the liability of that operator(s) to other designated operators under Union Acts.

Criterion 13.2

a) Banks are obliged to make sure that non-resident banks with which correspondent relations are established apply international AML/CFT standards (cl. 34 of the ICR of 23.05.2017 No. 2886). According to the amendments made on 17.03.2020 to the ICR No. 2886, when establishing and implementing correspondent relations with a non-resident bank, in addition to identifying a non-resident bank, the bank should:

- assess the AML/CFT measures applied by the non-resident bank;

- in respect of "transit accounts" - to receive appropriate confirmation of the respondent bank's fulfillment of the obligation to conduct due diligence in relation to its customers who have direct access to the correspondent bank's accounts, as well as of the possibility of providing the necessary data on the customer obtained as a result of identification at the request of the correspondent bank (cl. 33 of the ICR of 23.05.2017 No. 2886).

b) The requirements of this subcriterion are established in the ICR for banks (cl. 33 of the ICR of 23.05.2017 No. 2886). However, there are restrictions on the purpose of exchange of information between the banks (AML/CFT scope not included) in Article 14 of the Law of 30.08.2003 № 530-II "On bank Secrecy".

Criterion 13.3

1475. The requirements on prohibition to establish and continue relations with shell banks, application of measures aimed at prevention of establishing relations with non-resident banks, in respect of which there is information that their accounts are used by shell banks are partially established in the ICR regarding correspondent relations with non-resident banks (cl. 36, 45 of 23.05.2017 of the ICR No. 2886). In accordance with Article 14-20 of Law No. ZRU-580 of 05.11.2019, the operation of shell banks in the country is impossible, in this regard, there are no relevant requirements in terms of correspondent relationships with resident banks, which is not a deficiency.

Weighting and Conclusion

1476. The main elements are set in the Internal Control Rules for banks, separate ones for postal operators. There are the following deficiencies: postal operators are not obliged to study the AML/CFT measures of companies providing international money transfer services however, the legislation requires not to enter into a relationship with an operator that does not comply with AML/CFT measures (the weight of the disadvantage is insignificant); the Republic of Uzbekistan provided information on the impossibility of the functioning of shell banks on its territory. Considering the analysis of R.16 norms in relation to the sector of payment organizations (payment organizations, electronic money system operators and payment system operators), the country is proposed to extend the norms of R.13 to the operators of payment systems.

1477. **Recommendation 13 is rated Largely Compliant.**

Recommendation 14 - Money or value transfer services (MVTS)

1478. In the 2010 MER, the Republic of Uzbekistan was rated under SR. VI as "PC". The rating was due to the lack of information on legislative or other measures regarding money or value transfer services operating outside the formal financial system. Besides that, all the deficiencies noted in relation to AML/CFT measures in the banking and postal systems were also applicable in the context of money transfers.

1479. In the Republic of Uzbekistan, providers of payment services are Central Bank, banks, postal operators, payment organizations, as well as payment agents and subagents (Article 15 of Law of 01.11.2019 No. ZRU-578). The functioning of the payment system is ensured by the payment system operator, of the electronic money system by the electronic money system operator (Articles 7, 41 of the Law of 01.11.2019 No. ZRU-578).

Criterion 14.1

1480. In Uzbekistan, it is prohibited to provide money transfer services which covers the definition of MVTS in the FATF Glossary and captures transfers using a bank account, accepting cash for payments, using electronic money, and processing payments electronically and transmitting required information to FIs without an appropriate license from the Central Bank (Article 15 of the Law of 01.11.2019 No. ZRU-578).

1481. JSC "Uzbekiston Pochtasi" is the only postal operator involved in postal money transfers in the country and was created in accordance with Presidential Decree "On measures to reorganize and

improve the management of information systems" of 23.07.1997 No. UP-1823. The legislation does not provide for a separate requirement for the licensing of postal money order services. There is a general norm of Law "On Postal Communications" of 22.04.2009 No. ZRU-211 on the implementation of state regulation in the field of postal communications through licensing however, this provision does not disclose by whom and what entities are licensed, which is a minor deficiency.

Criterion 14.2

1482. The Central Bank has the ability to identify violations of the legislation on payments and payment systems during inspections. The legislation provides for both administrative and criminal liability for engaging in activities subject to licensing or obtaining other permits without a license.

1483. According to Article 165 of the CAO, engaging in activities subject to licensing or obtaining other permits without a license or other permits entails the imposition of a fine on citizens from 5 RSV (110 USD)[128] to 10 RSV (220 USD), and on officials - from 10 RSV (220 USD) to 20 RSV (440 USD). Engaging in activities without a license committed repeatedly within a year after the application of an administrative penalty, entails the imposition of a fine on citizens from 10 RCV (220 USD) to 20 RSV (440 USD), and on officials - from 20 RSV (440 USD) to 30 RSV (660 USD).

1484. According to Article 190 of the Criminal Code, engaging in activities subject to licensing, that is, without obtaining a special permit, associated with the receipt of income on a large scale, is punishable by a fine from 25 RSV (550 USD) to 75 RSV (1650 USD) or deprivation of a certain right up to five years or compulsory community service up to 300 hours or correctional labor up to 3 years. The same action committed on an especially large scale, by a dangerous recidivist or by prior conspiracy by a group of persons is punished with a fine from 75 RSV (1650 USD) to 100 RSV (2200 USD) or compulsory community service from 300 to 480 hours. The available sanctions in the CAO and CC are proportionate and dissuasive.

1485. A person who has committed an offence for the first time is released from liability if, within thirty days from the date of detection of the offence, he eliminated the consequences of engaging in activities without a license and compensated for the material damage caused.

1486. In the postal money order sector, the State Inspectorate for Control in the Field of Informatization and Telecommunications identifies, examines and checks business entities operating in the field of communications, informatization and telecommunications in violation of licensing requirements and conditions, as well as without obtaining an appropriate license. No sanctions have been established for activities without a license as there is no clear requirement for registration/licensing of this activity (see 14.1), which is a moderate disadvantage.

Criterion 14.3

1487. Banks and NBCIs, as well as organizations involved in money transfers, payments and settlements, are subject to the AML/CFT Law (Article 12).

1488. The Central Bank monitors and controls compliance by the licensed organizations with the AML/CFT ICR and the procedure for providing information related to AML/CFT to a specially authorized state body (Article 12 of Law of 11.11.2019 No. ZRU-582). Monitoring and control over compliance by operators and postal service providers with the ICR requirements are carried out by the State Inspectorate for Control in the Field of Informatization and Telecommunications, if necessary, in conjunction with a specially authorized state body (cl. 69 of the ICR of 28.08.2018 No. 3061).

Criterion 14.4

1489. In accordance with Article 19 of Law of 01.11.2019 No. ZRU-578, banks and payment organizations maintain registers of payment agents and payment subagents. The payment agent provides the bank or the payment organization with information about the engaged payment subagents for their inclusion in the specified register. The bank and the payment organization that have concluded agency agreements with the payment agent for the provision of payment services, shall submit to the Central

[128] The reference settlement value is equal to 223000 soums (clause 7 of Presidential Decree of 30.12.2019 No. PP-4555) or 22 USD at the rate of 20.04.2020.

Bank information about these services, as well as about their payment agents and subagents. According to the amendments made on 25.12.2020 to the ICR No. 2886, banks must maintain an updated register of their payment agents and payment subagents, available to competent authorities in the countries in which they, their agents and subagents operate (cl. 62 of the ICR of 23.05.2017 No. 2886).

1490. There is no requirement in the postal money order sector, since JSC "Uzbekiston Pochtasi" does not have agents providing postal money order services. There is no requirement for postal operators and providers.

Criterion 14.5

1491. In accordance with cl. 4 of the ICR of 30.06.2020 No. 3266 operators of payment systems, operators of electronic money systems and payment organizations, based on the requirements of the legislation and ICR, taking into consideration the activities of their payment agents and (or) payment subagents, shall without fail develop internal rules, which should reflect the procedure for interaction of payment agents and payment subagents with an officer responsible for AML/CFT internal controls.

1492. According to cl. 5 of the ICR of 30.06.2020 No. 3266, internal rules should be binding on payment agents and payment subagents. Thus, with regard to payment system operators, electronic money system operators and payment organisations, the requirement of this criterion has been met.

1493. With regard to postal service providers there are no such legal requirements to include agents in their AML/CFT programmes and to monitor their compliance with these programmes. In practice, there are no agents of Uzbekiston Pochtasi JSC, so the deficiency is minor.

Weighting and Conclusion

1494. There are the following deficiencies: there is no requirement in the legislation to license postal money order services, to apply sanctions for unlicensed activities in this sector, to maintain a register of payment agents and transfer it to the regulator. Taking into account the peculiarities of legislative regulation in the Republic of Uzbekistan of the postal remittance sector, namely the creation by Presidential Decree of the only state postal operator carrying out postal money transfers, which also has the status of designated operator for international postal communication in accordance with the acts of the Universal Postal Union, the identified deficiencies are insignificant.

1495. **Recommendation 14 is rated Largely Compliant.**

Recommendation 15 - New technologies

1496. In the 2010 MER, the Republic of Uzbekistan was rated under R.8 as "PC". The main deficiency was the weak specific AML/CFT regulation in relation to transactions using new technologies and transactions without personal presence, especially for financial institutions in the non-banking sector, and there were no requirements for managing ML/TF risks when using new technologies and conducting transactions without direct contact.

Criterion 15.1

1497. The risk assessment of new technologies at the country level is conducted at two levels: 1) when conducting a national ML/TF risk assessment; or 2) at the level of sectoral risk assessments in sectors where new financial and regulatory technologies are actively being introduced. For example, the 2019 national risk assessment took into account trends in remote banking (NRA, 2019, p.60), the introduction of online services by professional securities market participants (NRA, 2019, pp.70-71), and electronic exchange trading (NRA, 2019, p.73). The identification and assessment of the level of risks of new technologies was the basis for ML/TF risk assessment in the virtual asset turnover sector (SRA, 2020).

1498. FIs are obliged at least once a year to study, analyze and identify possible ML/TF/PF risks, record the results and take risk mitigation measures (Part 1 of Article 7 of the AML/CFT Law).

1499. The ICR prescribes the obligation to determine and assess the levels of risk in connection with new types of services and new business practices, using new or developing technologies for both new and existing types of services (banks - cl. 60 of the ICR of 23.05.2017 No. 2886, NBCIs - cl. 42 of ICR No. 2925 of 04.09.2017, the sector of payment organizations - cl. 35 of ICR No. 3266 of 30.06.2020, insurance companies - cl. 23^4 of the ICR of 03.11.2009 No. 2036, professional participants in the securities market - cl. 18^4 of the ICR of 03.11.2009 No. 2033, exchange members - cl. 29^1 of the ICR of 06.11.2009 No. 2038, leasing companies - cl. 194 of 22.09.2011 No. 2265, postal operators – cl.39 of the ICR of 28.08.2018 No. 3061 with amendments of 26.06.2021).

Criterion 15.2

a) From 28.03.2020, FIs, including NBCIs (cl. 42 of the ICR No. 2925 of 04.09.2017), must conduct a risk assessment before launching new types of services, business practices or using new or developing technologies (banks - cl. 61 of the ICR of 23.05.2017 No. 2886, sector of payment organizations - cl. 35 of the ICR No. 3266 of 30.06.2020, insurance companies - cl. 23^4 of the ICR of 03.11.2009 No. 2036, professional participants in the securities market - cl. 18^4 of the ICR of 03.11.2009 No. 2033, exchange members - cl. 29^1 of the ICR of 06.11.2009 No. 2038, leasing companies - cl. 194 of 22.09.2011 No. 2265, postal operators – cl.39 of the ICR of 28.08.2018 No. 3061).

b) The requirement to take measures to manage and mitigate risks associated with the use of new products, practices and technologies is established in the ICR for banks (cl. 61 of the ICR of 23.05.2017 No. 2886), sector of payment organizations - cl. 35 of the ICR No. 3266 of 30.06.2020, insurance companies (cl. 23^4 of the ICR of 03.11.2009 No. 2036), professional participants in the securities market (cl. 18^4 of the ICR of 03.11.2009 No. 2033), exchange members (cl. 29^1 of the ICR of 06.11.2009 No. 2038), NBCIs from 28.03.2020 (cl. 42 of the ICR No. 2925 of 04.09.2017), leasing companies - cl. 194 of 22.09.2011 No. 2265, postal operators – cl.39 of the ICR of 28.08.2018 No. 3061.

Criterion 15.3

a) The NAPM carried out a sectoral risk assessment of virtual assets circulation (approved by the decision of the IAC in April 2021). Based on the results of the analysis of the identified ML/TF risks, measures were proposed to minimize the risks and introduce a risk-based approach in the work of competent authorities, namely: NAPM Order No. 10/1 of 16.04.2021 on the risk-based approach was adopted, draft legislative acts were prepared and other planned activities are implemented.

b) According to the results of the SRA as one of the measures by the Law of the Republic of Uzbekistan of 05.10.2020 No. ZRU-640 "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan" VASPs are classified as subjects of financial monitoring. In particular article 12 of the AML/CFT Law was supplemented with paragraph thirteen with the following content: "persons involved in activities in the field of crypto assets turnover". In the Republic of Uzbekistan, activities in the field of circulation of virtual -assets are subject to licensing, including the creation of crypto-exchanges for trading crypto-assets (paragraph 4 of the Presidential Decree of 03.07.2018 № PP-3832). Thus, VASP in the context of the Republic of Uzbekistan is understood as a person carrying out any activity related to virtual assets, which covers the types of activities provided for by the FATF standards.

c) VASPs is subject to Article 7-1 of the AML/CFT Law, which ensures compliance with criteria 1.10 and 1.11. However, at the moment, only VASP, which carries out the activity of trade in VA, has been issued a license. Compliance with criteria 1.10 and 1.11 by VASPs in addition to the AML/CFT/CPF Law, is also based on the approved ICR for the corresponding category of reporting entities (cl. 14 of the Resolution of 09.06.2021 No. 3309).

Criterion 15.4

a) Activities of VASPs in the field of virtual assets turnover, including the establishing of crypto exchanges for trading in crypto assets in the territory of the Republic of Uzbekistan are subject to licensing (cl. 4 of Presidential Decree of 03.07.2018 No. PP-3832). Activities as VASPs in the field of circulation of virtual assets, based on the aforementioned general norm, are also subject to licensing. That is, at present any activity of physical persons as VASPs is recognized as unlicensed and, therefore, illegal.

b) The ICR for persons engaged in circulation of virtual assets contains a provision on exclusion of criminals and their accomplices in the management of VASPs (cl. 8 of Decree of 9.06.2021 No. 3309). However, this requirement does not apply to founders and the beneficial ownership of VASP which is a significant shortcoming. The licensing authority is taking measures of an operational nature and interaction, including with foreign partners, to prevent the penetration of criminals into the possession of VASP, but they were not disclosed to the team of assessors and supporting documents are not presented due to confidentiality.

Criterion 15.5

1500. The licensing authority (NAPM - cl. 4 of Presidential Decree of 03.07.2018 No. PP-3832, cl. 2 of Regulation of 22.01.2019 No. 3127) has the right to send to the relevant authorities materials on the revealed facts of carrying out activities by crypto exchanges without a license to take measures stipulated by law (for the sanctions imposed for activities without a license, see Criterion 14.2). During the period 2019-2020, the Agency detected 6 cases of unlicensed activities, which were sent to the GPO and the STC and resulted in 4 criminal cases, as well as 9.5 bitcoins were recovered in one of the criminal cases. Detection of the facts of VASPs activities without a license is carried out by: monitoring the Internet resources, social networks and messengers; maintaining a special e-mail NAPM fraud@napm.uz to receive information from the public on the facts of fraudulent schemes in the area of VA circulation; information exchange with law enforcement agencies; conducting explanatory work among citizens and entrepreneurs, during which we receive information and applications about suspicious actors who offer to commit illegal actions or get rich at the expense of virtual assets.

Criterion 15.6

a) NAPM and other authorized bodies exercise control over the activities of VASPs in terms of their compliance with the AML/CFT legislation (cl. 2 of Presidential Decree No. 3926 of 02.09.2018). A number of licensing requirements have been established, including the "Rules for the implementation of crypto exchange trading" (cl. 3 of Presidential Decree of 02.09.2018 No. 3926); based on the results of the SRA, NAPM Order No. 10/1 of April 16, 2021 on the risk-based approach was adopted. The Agency's supervision of virtual assets is carried out considering the identified risks. In particular, monitoring of the Internet resources, social networks and messengers has been strengthened, as a result 6 information resources on provision of illegal sale and purchase of virtual assets services were identified. In order to prevent the involvement of citizens, an information message was prepared and published (http://napm.uz/ru/press_center/news/informatsionnoe-soobshchenie-natsionalnogo-agentstva-proektnogo-upravleniya-pri-prezidente-respublik). Subsequently, given that these resources were placed and registered abroad at the request of NAPM, the authorized bodies blocked these 6 information resources.

b) The NAPM has all the necessary supervisory powers, including conducting inspections, requesting information, imposing sanctions, limiting and revoking a license (cl. 31 of Regulation of 22.01.2019 No. 3127). The deficiencies indicated in R.27 do not apply to this criterion because the powers of the NAPM are regulated by a separate law.

Criterion 15.7

1501. As a guide, there is a document "Rules for the implementation of crypto exchange trading" (as an Annex to Regulation of 01.22.2019 No. 3127). The ICR No. 3309 of 09.06.2021 was adopted, which, inter alia, in Chapter 5 defines the criteria and characteristics of suspicious transactions, as well as the procedure for their detection. There is no information about other guidelines to assist VASPs in the implementation of AML/CFT measures, as well as information on provision of the feedback regarding the STRs. This is due to the objective reason for the non-functioning of VASPs to date. As a feedback, the country demonstrated the explanatory work carried out by the NAPM in the form of press conferences, publications about the high risk of involving the population in illegal schemes with the IA. For example, in 2021 3 training via videoconference were held, at which the requirements of AML/CFT regulations were explained to VASPs, the main risks were outlined. Also, a number of

articles were organized in the media to explain to citizens the basics of VA turnover and the need to improve digital literacy.

Criterion 15.8

a) In addition to sanctions for non-compliance with licensing requirements (cl. 33, 34 of Regulation of 22.01.2019 No. 3127), Article 179-3 of the CAO provides for sanctions for non-compliance with the requirements of AML/CFT legislation: imposition of a fine from 15 RSV (330 USD)[129] to 30 RSV (660 USD), repeated commission of the offence within a year after the application of an administrative penalty entails the imposition of a fine from 30 RSV (660 USD) to 50 RSV (1100 USD). These sanctions are proportionate and dissuasive based on the size of the average nominal wage (as of Q3 2019 according to the State Statistics Committee) in the Republic of Uzbekistan, which is 2,217,827 sums, or $231, taking into account the dollar-to-sum exchange rate as of Q3 2019.

b) The legislation does not establish clear grounds for applying sanctions to directors and senior managers of VASPS. At the same time, according to the ICR, managers of persons engaged in circulation of virtual assets and the responsible employee shall be liable for violation of the ICR in accordance with the legislation (cl. 58 of the Decree No. 3309 of 9.06.2021).

Criterion 15.9

1502. In accordance with the legislation (AML/CFT Law, ICR) the obligations for VASPs to comply with the requirements set out in Recommendations 10-21 are partially established. R.10 is implemented with the following proviso, as established by the FATF Standards: the requirements and thresholds when to conduct CDD are established in the ICR for the persons engaged in circulation of virtual assets (p.19 of the Decision No. 3309 of 9.06.2021), including when carrying out single transactions with the amount exceeding the equivalent of USD 1000 on the date of transaction (15.9.a).

1503. There are the following shortcomings:

- Recommendation 10: legislation does not establish requirements for understanding the business of a legal entity and the ownership structure of that legal entity (10.8); the obligation to recognize the head of a legal entity as the beneficial owner is not established (10.10); no requirement to identify the beneficial owner of foreign trusts is established (10.11); there is no requirement to use simplified identification measures in low-risk cases (10.17-10.18).
- Recommendation 11: the legal requirement does not fully cover the FATF requirements (ensure storage of information on both domestic and international transactions, ensure storage of the results of any analysis conducted) (11.1-11.2).
- Recommendation 12: the requirements do not apply to the national PEPs.
- Recommendation 16: Uzbekistan has not imposed R.16 requirements for VASPs (15.9. b) because no entities are yet licensed to be allowed to make electronic VA transfers.
- Recommendation 18: there is no requirement to have an independent auditing system.

Criterion 15.10

1504. From 05.10.2020, the AML/CFT Law classifies VASPs as organizations involved in transactions in monetary funds and other assets. The legislation contains provisions prohibiting legal entities to provide access directly or indirectly to funds or other property, material resources, financial and other services to persons included in the list of persons participating or suspected of participating in terrorist activities, as well as to persons acting on their behalf (cl. 2 of the General Prosecutor's Order of 11.10.2016 No. 2833). Crypto exchanges are not entitled to establish relations with persons included in such a list of persons (cl. 11 of Regulation of 22.01.2019 No. 3127). The DCEC provides the List to the licensing authorities, and the licensing authorities provides it to the organizations involved in transactions in monetary funds and other assets (cl. 21 of the General Prosecutor's Order of

[129] The RSV is equal to 223,000 soums (point 7 of Presidential Decree No. PP-4555 of 30.12.2019) or 22 USD at the exchange rate on 20.04.2020.

11.10.2016 No. 2833). Detailed analyzes are provided in R.6 and 7 (6.5 (d), 6.5 (e), 6.6 (g), 7.2 (d), 7.2 (e), 7.3 and 7.4 (d), taking into consideration the deficiencies noted in 6.5 (b)).

Criterion 15.11

1505. In Uzbekistan, there is a legal basis for the exchange of information with foreign partners, regardless of the nature or status of the supervisory authorities and differences in the nomenclature or status of VASPs (cl. 5 of Presidential Decree of 27.07.2017 No. PP-3150). In accordance with point 6 of the Regulation on the procedure for international cooperation in the field of AML/CFT/PF, approved by Cabinet of Ministers Decision No. 402 of 29.06.2021, NAPU is classified as a supervisory body and is subject to the exchange of supervisory information relevant to AML/CFT objectives in accordance with criteria 40.12 - 40.16.

1506. International cooperation is carried out in accordance with the analysis of R.37 - R.40.

Weighting and Conclusion

1507. The requirements for evaluating new technologies are fully implemented. Certain FATF requirements in regard to VASPs, in particular on licensing, customer identification, information storage and international cooperation, have been implemented into legislation. However, there are deficiencies: there are no requirements to prevent criminals and their accomplices from entering the VASP beneficial ownership; there is no direct requirement for applying sanctions not only to VASPs, but also to their directors and senior managers.

1508. **Recommendation 15 is rated Largerly Compliant.**

Recommendation 16 – Wire transfers

1509. In the MER 2010, the Republic of Uzbekistan was rated under SR. VII as "PC". There were no requirements to maintain information about the originator; banks are not obliged to consider limiting or terminating business relationships with financial institutions that do not comply with SR.VII requirements; there were no special measures to monitor financial institutions' compliance with the wire transfer rules; there is no requirement for all intermediary financial institutions to transfer information about the originator along the transfer chain; there were no risk management procedures for transfers that are not accompanied by information about the originator, including filing information to the FIU; there were no procedures for considering termination of relations with the ordering financial institution.

Criterion 16.1

1510. Banks, postal operators and payment organisations are obliged to accompany international wire transfers of natural persons with information about the originator and beneficiary of the transfer in accordance with the FATF requirements (cl. 38 of the ICR of 23.05.2017 No. 2886; Article RP 703 of the Postal Payment Services Agreement and its Regulations, cl. 30 of ICR No. 3266 of 30 June 2020). Obligation to record information about the originator and beneficiary legal entity is also available (paragraph 18 of the Regulations on the procedure of electronic payments through the interbank payment system of the Central Bank from 14.02.2006 № 1545, (cl. 83 of the Rules for the provision of postal services of 18.04.2011 No. 2219, cl. 30 of ICR for payment organizations No. 3266 of 30 June 2020).

1511. However, there are very limited exceptions in the law, which are a moderate shortcoming in meeting the requirement of this criterion. Banks are not required to apply CDD measures and, accordingly, to accompany transfers between individuals with information about the sender when carrying out transactions with the use of bank cards for an amount less than 300 times the basic settlement amount (about 6-7 thousand US dollars); as well as when paying for utilities, communication services, payments to the budget, extra-budgetary funds and other obligatory payments (paragraph 22 of the ICR of 23.05.2017 № 2886).

1512. Payment organizations sector (payment organisations, electronic money system operators and payment system operators) do not conduct customer CDD and, therefore, have no information about them to accompany the transfer in the following case (cl. 17 of the ICR of 30.06.No. 3266):

- when the maximum amount of one transaction carried out by an individual who is the owner of electronic money does not exceed the amount equal to the basic settlement amount.

Criterion 16.2

1513. The Uzbekistan legislation does not deal separately with "batch transfers". When receiving separate wire transfers from one originator to different beneficiaries, each of them is conducted separately without sending batch files. There are also deficiencies noted in Criterion 16.1.

Criterion 16.3

1514. The Republic of Uzbekistan in limited circumstances apply the minimum threshold in accordance with Criterion 16.1, when money transfers are not accompanied by the required information about originators.

Criterion 16.4

1515. The ICR for banks, payment organizations sector and postal operators have general rules on conducting CDD if there is suspicion of ML/TF (cl. 22 of the ICR of 23.05.2017 No. 2886, cl. 20 of the ICR No. 3266 dated June 30, 2020, cl. 18 of the ICR of 28.08.2018 No. 3061).

Criterion 16.5

1516. According to the amendments made on 17.03.2020 to the ICR No. 2886 for banks, data on domestic wire transfers must include information about the originator, as prescribed for international wire transfers (cl. 38-1 of the ICR of 23.05.2017 No. 2886).

1517. In accordance with cl. 83 of the Rules for the provision of postal services of 18.04.2011 No. 2219, these requirements apply to both international and domestic wire transfers. In cl. 30 of the ICR No. 3266 of 30.06.2020 such requirement is established for payment organizations. There is no similar requirement for electronic money system operators and payment system operators.

1518. Nevertheless, in a number of cases specified in cl. 22 of ICR No. 2886 dated May 23, 2017 and cl. 17 of ICR No. 3266 dated June 30, 2017, CDD is not conducted and bank and payment organization have no data on clients to support funds transfers.

Criterion 16.6

1519. In Uzbekistan, the originator and beneficiary information not always accompanies the transfer that said no other means are used (see Criterion 16.5).

Criterion 16.7

1520. The general norm of Article 21 of the AML/CFT Law and ICR for banks and postal operators apply (see the analysis of R.11).

Criterion 16.8

1521. There are direct rules in the legislation obliging the ordering financial institution (banks, payment organisations sector and postal service providers) to refuse to conduct a wire transfer (international and domestic) if it does not meet the requirements specified above in the Criterion 16.1-16.7.

1522. According to the amendments made on 17.03.2020 to the ICR No. 2886, banks are prohibited from providing money transfer services, including through international money transfer systems, if the wire transfer does not meet the established requirements (cl. 38 of the ICR No. 2886 of 23.05.2017). A similar amendment has been made to the ICR of payment organisations and postal service providers (cl. 31 ICR No. 3266 of 30.06.2020, cl. 23-1 ICR No. 3061 of 28.08.2018). There is no similar requirement for electronic money system operators and payment system operators.

Criterion 16.9

1523. Banks acting as an intermediary (transit bank) in a wire transfer must ensure the transfer and keeping for at least five years of all records on the originator and beneficiary accompanying the electronic transfer, together with the transfer (cl. 40 of the ICR of 23.05.2017 No. 2886). Payment organizations, when providing services on acceptance and execution of money transfers through money transfer systems, including when they act through their payment agents (subagents), must ensure that sent money transfers are accompanied by accurate information about the sender client and the recipient (paragraph 30 of the ICR № 3266 of June 30, 2020). The ICR for postal operators does not contain similar rules for an intermediary institution. Uzbekistan provided information that the functions of an intermediary institution are not carried out by the postal operator JSC "Uzbekiston Pochtasi".

Criterion 16.10

1524. Obligations to keep records and to archive information by intermediary banks apply to all bank transfers, including in cases where technical restrictions prevent archiving all required information on the originator and beneficiary. There is no similar requirement for payment organisations, electronic money system operators and payment system operators.

Criterion 16.11

1525. Banks, postal operators, payment organizations are obliged to take reasonable and accessible measures to identify international wire transfers that do not have the required information about the beneficiary and (or) the originator (cl. 40 of the ICR of 23.05.2017 No. 2886, cl. 23-1 of the ICR dated 28.08.2018 No 3061, cl. 30 of the ICR No 3266 of 30.06.2020). Uzbekistan did not provide the required information for operators of electronic money systems and payment system operators.

Criterion 16.12

1526. Banks, postal operators, payment organizations sector are obliged, on the basis of a risk assessment, to develop an internal document establishing the procedure for the implementation of measures (for execution, declining, suspension, etc.) in the event of identifying international wire transfers that do not have the required information about the beneficiary and (or) the originator (cl. 40 of the ICR of 23.05 .2017 No. 2886, cl. 23-1 of the ICR dated 28.08.2018 No 3061, cl. 30 of the ICR No 3266 of 30.06.2020). Banks, the payment institution sector and postal service operators should develop such a document based on a risk assessment. For banks, the payment institution sector and postal operators, there is no follow-up procedure.

Criterion 16.13

1527. Banks, payment organizations and postal operators are obliged to take reasonable and accessible measures to identify international wire transfers that do not have the required information on the beneficiary and (or) the originator (cl. 38 of the ICR of 23.05.2017 No. 2886, cl. 30 of the ICR No 3266 of 30.06.2020, cl. 13 of the ICR of 28.08.2018 No. 3061).

Criterion 16.14

1528. There is no clear requirement for recipient banks to verify the beneficiary's personal data in cross-border wire transfers. There is a general requirement for banks to carry out money transfer operations after CDD in relation to individuals (cl. 38 of the ICR of 23.05.2017 No. 2886, cl. 30 of the ICR No 3266 of 30.06.2020). Banks are required to keep information on transactions for at least 5 years (cl. 89 of the ICR of 23.05.2017 No. 2886). Postal operators shall check the beneficiary's personal data during a cross-border wire transfer and keep the relevant information for at least 5 years (cl. 121 of the Annex to Order of the General Director of the Agency for Communications and Informatization of 18.04.2011 No. 2219). Considering that CDD measures imply verification and this procedure does not depend on threshold amounts, the absence of a clear requirement for verification is considered as minor shortcoming.

Criterion 16.15

1529. Banks and postal operators are obliged to develop an internal document or rules establishing the procedure for implementing measures in case of detecting international wire transfers that do not have the required information about the beneficiary and (or) the originator (cl. 38 of the ICR of 23.05.2017 No. 2886, cl. 4 of the ICR No 3266 of 30.06.2020, cl. 13 of the ICR of 28.08.2018 No. 3061). Such measures can be execution, declining, suspension of the transfer. Such a document is developed based on the risk assessment which meet requirement of this criterion.

1530. But, there is no follow-up procedure for banks, sectors of payment organizations and postal operators.

Criterion 16.16

1531. In the Republic of Uzbekistan, payment service providers are banks, postal operators, payment institutions, as well as payment agents and subagents (Article 15 of the Law of 01.11.2019 No. ZRU-578). The requirements for compliance with R.16 in countries where banks and the payment institution sector operate directly or through agents are met except for the following (cl. 38 of the ICR of 23.05.2017 No. 2886, cl. 4 and 5 of the ICR No 3266 of 30.06.2020). The legislation does not specify that these requirements should be applied to foreign offices and departments. There are no relevant requirements for postal operators.

Criterion 16.17

1532. According to the amendments made on 25.12.2020 to the ICR No. 2886, banks, in the event that they serve both the originator and the beneficiary of a wire transfer, must:

- take into consideration all information received from both the originator and the beneficiary to determine whether it is necessary to file a suspicious transaction report;
- file a suspicious transaction report to competent authorities in any country with which the suspicious money transfer is associated, and provide the relevant information about the wire transfer (cl. 391 of the ICR of 23.05.2017 No. 2886).

1533. The requirements of this criterion are also set out in the ICR for payment organisations, operators of electronic money systems (cl. 40 of ICR No. 3266 of 30.06.2020).

1534. According to information provided by the country, JSC "Uzbekiston Pochtasi" controls either the originator or the beneficiary of a wire transfer. At the same time, for the operators of payment systems that control both the originator and the beneficiary of a wire transfer, and for the postal operators, the relevant requirements have not been established.

Criterion 16.18

1535. FIs are obliged to check the participants in the operation against the list of persons involved or suspected of involvement in terrorist activities or the proliferation of weapons of mass destruction, and are also obliged to suspend the operation without delay and without prior notice, with the exception of operations for crediting funds to the account of a legal or natural person, and (or) freeze money or other property of persons designated in the list of persons involved or suspected of involvement in terrorist activities or the proliferation of weapons of mass destruction (Article 15 of the AML/CFT Law; cl. 3 of the Annex to the General Prosecutor's Order of 11.10.2016 No. 2833; cl. 52 of the ICR of 23.05.2017 No. 2886; cl. 50, 51 of the ICR of 28.08.2018 No. 3061, cl. 29 and 41 of the ICR No 3266 of 30.06.2020). The withdrawal on the receipt of funds in the account indicates that the operation is not suspended, the funds are credited to the account and frozen.

Weighting and Conclusion

1536. Uzbekistan has implemented the requirements of this Recommendation on international money transfers of individuals, on information of intermediary financial institutions on wire transfers in terms of freezing transfers of persons designated in the list. The following minor deficiencies were identified: there are very limited exemptions in the legislation on the amounts and cases when money transfers and electronic money transfers are not accompanied by the required sender and recipient

information; in Uzbekistan information about the originator and beneficiary does not always accompany the transfer, while other means are not used; there is no procedure for follow-up in case of detection of money transfers without the required beneficiary and (or) originator information, for postal operators no requirements to perform R.16 in countries where they carry out their activities directly or through agents.

1537. **Recommendation 16 is rated Largerly Compliant.**

Recommendation 17 - Reliance on third parties

1538. In the 2010 MER, the Republic of Uzbekistan was rated under R.9 as "NC".

1539. Banks, NBCIs, exchange members, payment organizations, electronic money system operators, payment system operators, postal service operators can rely on third parties in the implementation of clauses (a) - (c) of CDD measures provided for in R.10 (cl. 232 of the ICR of 23.05.2017 No. 2886, cl. 221 of the ICR of 04.09. 2017 No. 2925, cl. 19 of the ICR of 30.06.2020 No 3266, cl. 16-3 of the ICR of 6.11.2009 No 2038, cl. 20-1 of the ICR No 3061 of 28.08.2018). It also states that in such cases, the ultimate responsibility for proper customer due diligence falls on the FIs themselves. However, there is no relevant instruction for payment organizations, electronic money system operators, payment system operators in the ICR.

Criterion 17.1

a) FIs can only rely on the results of CDD conducted by a third party if they are sure that they can immediately receive (through electronic systems) the required CDD information. In case of non-compliance with this requirement, FIs are obliged to independently take CDD measures of (cl. 232 of the ICR of 23.05.2017 No. 2886, cl. 221 of the ICR of 04.09.2017 No. 2925, cl. 16-3 of the ICR of 6.11.2009 No. 2038, cl. 19 of the ICR of 30.06.2020 No. 3266, 20-1 of the ICR of 28.08.2018 No. 3061).

b) FIs can only rely on the results of third party CDD if they are sure that they can without delay obtain copies of identification data and other relevant CDD documents upon request. In case of non-compliance with this requirement, FIs are obliged to independently take CDD measures (cl. 232 of the ICR of 23.05.2017 No. 2886, cl. 221 of the ICR of 04.09.2017 No. 2925, cl. 16-3 of the ICR No. 2038 of 6.11.2009, cl. 19, 40 of the ICR No. 3266 of 30.06.2020, cl. 20-1 of the ICR No. 3061 of 28.08.2018).

c) FIs can rely on the results of CDD conducted by a third party only if they are sure that the third parties are governed by the AML/CFT/CPF internal rules (cl. 232 of the ICR of 23.05.2017 No. 2886, cl. 221 of the ICR of 04.09.2017 No. 2925, cl. 19 of the ICR of 30.06.2020 No. 3266, cl. 16-3 of the ICR of 6.11.2009 No. 2038).

Criterion 17.2

1540. The ICR of the above-mentioned FI states that third parties are organizations registered in the Republic of Uzbekistan and carrying out transactions with funds or other property, specified in Article 12 of the Basic Law of the Republic of Uzbekistan. Thus, it is not allowed to rely on third parties outside of Uzbekistan.

Criterion 17.3

1541. The AML/CFT law and the ICR do not distinguish between a third party, which is a member of the group or an external party, therefore this criterion is applicable to financial groups operating within the country. However, the criterion is not applicable to financial groups operating abroad (having foreign branches and subsidiaries). However, the shortcomings reflected in R.18 apply to financial groups operating domestically.

Weighting and Conclusion

1542. In general, the requirements of R.17 are met, but there is no indication in the ICR of payment organizations, electronic money system operators, payment system operators that when relying on

third parties, the ultimate responsibility for customer due diligence is borne by the organizations themselves.

1543. **Recommendation 17 is rated Largerly Compliant.**

Recommendation 18 - Internal controls, foreign branches and subsidiaries

1544. In the MER 2010, the Republic of Uzbekistan was rated under R.15 as "PC". Regarding R.15, the main deficiencies were related to the absence of a requirement for mandatory training of employees of financial institutions on AML/CFT issues and the lack of standards for such training; the absence of a requirement for mandatory verification of employees of financial institutions when hiring and carrying out activities. The requirements of Recommendation 22 have not been implemented into legislation.

Criterion 18.1

1545. FIs are obliged to organize and implement internal control systems (Article 15 of the AML/CFT Law). The AML/CFT ICR for FIs shall be developed and approved by the relevant supervisory, licensing and registration authorities in conjunction with a specially authorized state body, and in the absence of such, with a specially authorized state body (Article 6 of the AML/CFT Law). When developing internal rules or introducing an internal control system, financial institutions should take into consideration the specifics of functioning and the level of risks (banks - cl. 5.7 of the ICR of 23.05.2017 No. 2886, NBCIs - cl. 6 of the ICR of 04.09.2017 No. 2925, insurance companies - cl. 5 of the ICR of 03.11.2009 No. 2036, professional participants in the securities market - cl. 7 of the ICR of 03.11.2009 No. 2033, postal operators - cl. 4 of the ICR of 28.08.2018 No. 3061, exchange members - cl. 7 of the ICR of 06.11.2009 No. 2038, leasing companies - cl. 5 of the ICR of 22.09.2011 No. 2265, the sector of payment organizations - cl. 4 of the ICR of 30.06.2020 № 3266).

a) The AML/CFT ICR for FIs provides for establishing an internal control system or internal rules. In financial institutions, the appointment of an official at the management level for ensuring compliance with requirements in the AML/CFT field is limited to the level of the head of the internal control service, the head of the unit, the person in charge, and the controller.

b) Requirements for the qualifications and business reputation of the FI employees (except for employees of internal control units, heads of banks and NBCIs, controllers of professional securities market participants) are not established. Requirements for the qualifications and business reputation of persons in charge of AML/CFT in the exchange trading sector and leasing organizations are established in ICR (cl. 9-1 of Decree № 2038 of 06.11.2009 and cl. 4 of the ICR of 22.09.2011 No. 2265). There are no requirements for their business reputation.

c) The ICR for financial institutions (except for exchange members and leasing organizations) provide for regular retraining of employees (banks - cl. 20 of the ICR of 23.05.2017 No. 2886, NBCIs - cl. 20 of the ICR of 04.09.2017 No. 2925, insurance companies - cl. 13, 14 of the ICR of 03.11.2009 No.2036, professional participants in the securities market - cl. 6 of the ICR of 03.11.2009 No. 2033, postal operators - cl. 16 of the ICR of 28.08.2018 No. 3061). The Internal Control Rules for exchange members and leasing organizations provide only training for the responsible person on AML/CFT (cl. 14 of the ICR of 06.11.2009 No. 2038, cl. 12 of the ICR of 22.09.2011 No. 2265).

d) Internal audit of AML/CFT systems has been established for banks and NBCIs (cl. 99, 100 of the ICR of 23.05.2017 No. 2886; cl. 74 of the ICR of September 4, 2017, No. 2925). The possibility of monitoring the effectiveness of the internal control system by the internal audit service (if any) is defined for exchange members, postal operators, leasing organizations.

Criterion 18.2

1546. According to the amendments made on 17.03.2020 to the ICR No. 2886, the internal rules of a banking group shall include:

a) the rules and procedures for the exchange of data necessary to manage AML/CFT/CPF risks and apply CDD;

b) ensuring at the level of the group of compliance control, audit and (or) AML/CFT/CPF functions, obtaining, in cases necessary for the purposes of AML/CFT/CPF, information from branches and subsidiaries on their customers, accounts and operations;

c) protection of confidentiality and data use at a sufficient level (cl. 6-1 of the ICR of 23.05.2017 No. 2886).

1547. There are no similar requirements for other financial groups.

Criterion 18.3

1548. Banks, NBCIs, sector of payment organizations, insurance companies, exchange members, professional participants in the securities market and leasing organizations are obliged to require their foreign separate subdivisions to inform the head office if it is impossible to apply appropriate AML/CFT measures due to the existing prohibition by the laws of the country in which their separate subdivisions are located. When implementing AML/CFT measures, foreign separate subdivisions of these financial institutions must comply with the internal rules of the parent organization, if the legislation of the host country provides for less stringent AML/CFT measures than the AML/CFT measures of the parent organization (cl. 36 of the ICR of 23.05.2017 No. 2886, NBCIs - cl. 34 of the ICR of 04.09.2017 No. 2925, sector of payment organizations - cl. 15 of the ICR No. 3266 of 30.06.2020, insurance companies - cl. 5, 51 of the ICR of 03.11.2009 No. 2036, exchange members - cl. 7-1, 7-2 of the ICR of 06.11.2009 No. 2038, professional participants in the securities market - cl. 16-2, 16-3 of the ICR of 03.11.2009 No. 2033, leasing organizations - cl. 19-5 of the ICR of 02.09.2009 No. 2265). There are no requirements for a postal operator. JSC "Uzbekistan Pochtasi" has no foreign branches and foreign subsidiaries.

Weighting and Conclusion

1549. In Uzbekistan, the system of internal control of financial institutions is organized taking into consideration the specifics of functioning, activities and the level of risks. Banks and other large financial institutions create structural divisions for AML/CFT, whose employees have requirements for qualifications and business reputation. Most FIs conduct regular retraining of employees. The following moderate deficiencies were identified: in financial institutions, the AML/CFT official does not belong to the management team and for the main FI is limited to the position of the head of the internal control service; there are no requirements for the qualifications and business reputation of the FI employees (except for AML/CFT units, heads of banks and NBCIs); there are no requirements for business reputation of AML/CFT responsible persons for exchange members and leasing organizations; internal audit of AML/CFT systems is established only for banks and NBCIs; FIs (except for banks) do not use group AML/CFT programmes.

1550. **Recommendation 18 is rated Partially Compliant.**

Recommendation 19 – Higher risk countries

1551. In the 2010 MER, the Republic of Uzbekistan was rated under R.21 as "LC", since it was not possible to assess the effectiveness of the measures taken.

Criterion 19.1

1552. All FIs are required under their ICRs to apply enhanced CDD measures to business relationship and transactions with natural and legal persons (including FIs) from countries for which this is called for by the FATF. The risk of such customers is considered high under the FI's CDD, but may be reviewed as the nature of their transactions changes .

Criterion 19.2

1553. Countermeasures are being applied in Uzbekistan. Thus, all persons permanently residing, staying or registered in a State that is not participating in international cooperation in the field of AML/CFT,

and their operations are assessed as high-risk operations, and FIs file STRs concerning them to the DCEC. Transactions in monetary funds and other assets (performed and prepared) are subject to reporting to the DCEC, if one of the parties is a person permanently residing, staying or registered in a State not participating in international cooperation in the field of AML/CFT (Article 13 of the AML/CFT Law). The legislation does not contain provisions on the application by financial institutions (with the exception of banks and NBCIs) of countermeasures specified in the Interpretive Note to R.19 when called for by the FATF or regardless of any call of the FATF, with the exception of the enhanced CDD (see Criterion 19.1) and special control over the operations of these persons.

Criterion 19.3

1554. The DCEC makes lists of States that do not participate in international cooperation in the field of combating money laundering and terrorist financing, and for which relevant international organizations have called for measures to protect the international financial system from ML/TF/CPF risks and provides them to organizations with subsequent notification of the changes introduced. This information is communicated through the Department of Methodology, Risk Assessment and Typologies of the Department for Combating Money Laundering and Financing of Terrorism (cl. 2.2 of the Regulation on the Department of International Relations of the Department for Combating Money Laundering and Financing of Terrorism, approved by Order № 27 of the Head of the Department for Combating Money Laundering and Financing of Terrorism dated 30.06.2018).

Weighting and Conclusion

1555. FIs apply enhanced CDD measures to individuals from jurisdictions with high AML/CFT risks. However, possible countermeasures for FIs (with the exception of banks and NBCIs) have not been developed against States that do not participate in international cooperation in the field of AML/CFT, with the exception of filing STRs and applying CDD measures. There is no statutory requirement to apply enhanced CDD measures commensurate with the risks.

1556. **Recommendation 19 is rated Largely Compliant.**

Recommendation 20 – Reporting of suspicious transactions

1557. In the 2010 MER, the Republic of Uzbekistan was rated under R.13 and SR.IV as "LC". The main deficiencies were related to the effectiveness of the implementation of R.13 requirements due to the lack of ML criminalization, as well as the low number of STRs, indicating the low effectiveness of the STR system as a whole.

Criterion 20.1

1558. FIs are required to file an STR to a designated government authority if there is suspicion, based on the criteria and indications of dubiousness that a transaction being conducted or prepared is for ML/TF/PF purposes (Art. 13 of the AML/CFT Law). There are no restrictions on filing STRs for predicate offenses in the law of the land. The ICR for FIs also specifies that FIs may treat a transaction as suspicious if there are grounds or circumstances (in the case of insurance and leasing companies) for suspicion of ML/TF/PF (banks – cl. 49-51 of the ICR of 23.05.2017 No. 2886; NBCIs – cl. 36, 37 of the ICR of 04.09.2017 No. 2925; insurance companies – cl. 25 of the ICR of 03.11.2009 No. 2036; postal operators – cl. 40 of the ICR of 28.08.2018 No. 3061; professional participants in the securities market – cl. 19 of the ICR of 03.11.2009 No. 2033; exchange members – cl. 30 of the ICR of 06.11.2009 No. 2038; leasing companies – cl. 21 of the ICR of 22.09.2011 No. 2265, payment organizations sector - cl. 20 of the ICR of 30.06.2020 No. 3266). FIs file STRs to a special authorized state body no later than one business day following the day of detection of such a transaction (Art. 15 of the AML/CFT Law). Such body is the DCEC (cl. 1 of the Decree of the President of the RU of 23.05.2018 No. UP-5446).

Criterion 20.2

1559. FIs are obliged to file STRs to a specially authorized state body, including reports on attempts to commit such transactions, in the prescribed manner no later than one business day following the day of their detection (Art. 15 of the AML/CFT Law). There are no reservations as to the amount of such transactions.

Weighting and Conclusion

1560. **Recommendation 20 is rated Compliant.**

Recommendation 21 – Tipping-off and confidentiality

1561. In the 2010 MER, Uzbekistan was rated under R.14 as "PC" due to the lack of an express prohibition on disclosure of the fact that STRs or related information is to be filed or have been provided to the FIU.

Criterion 21.1

1562. The provision by FIs in due course of information on transactions in monetary funds or other assets of legal entities or individuals or other information to a specially authorized state body is not a violation of commercial, banking or other secrets protected by law (Art. 18 of the AML/CFT Law). At the same time, there is no direct indication in the legislation that the provision of information cannot be a basis for liability regardless of whether it was known exactly what the previous criminal activity was, as well as whether the illegal activity actually took place.

Criterion 21.2

1563. FIs are prohibited from disclosing the fact that STRs or other information are sent to the FIU (Articles 19, 20 of the AML/CFT Law). , and FIs themselves must ensure that access to information related to AML/CFT/CPF is restricted (Art. 20 of the AML/CFT Law).

Weighting and Conclusion

1564. The Republic of Uzbekistan has taken all the basic measures, but the lack of a direct indication in the legislation that the provision of information cannot be the basis for liability regardless of whether the illegal activity actually took place, carries risks associated with the emergence of liability of the organization or its employees to third parties.

1565. **Recommendation 21 is rated Largely Compliant.**

Recommendation 22 – DNFBPS: customer due diligence

1566. In the 2010 MER, Uzbekistan was rated under R.12 as "NC". The main deficiencies were the lack of AML/CFT requirements in the context of identification, verification and CDD measures, as well as data archiving and the lack of a control mechanism for complex, unusual and particularly large operations and transactions.

1567. DNFBPs in Uzbekistan include organizations conducting lotteries and other risk-based games; precious metals and stones dealers; persons providing services and participating in transactions related to the purchase and sale of real estate (hereinafter – realtors); notary offices, lawyers' groups and audit organizations – when preparing and conducting transactions on behalf of customers (Art. 12 of the AML/CFT Law).

Criterion 22.1

1568. The application of CDD measures is regulated in the relevant ICRs. For most categories of DNFBPs there is no indication of what information is established when verifying the identity of the beneficial owner (except for the audit sector); no obligation to conduct CDD (update data) on existing customers when national CDD requirements change; all DNFBPs, other than auditors and precious metals and stones dealers, are not required to consider the need to file an STR when CDD measures cannot be

properly applied (Criterion 10.19); there is no rule allowing an STR to be filed instead of conducting CDD when there is a risk of disclosure to a customer (Criterion 10.20).

a) Not applicable due to the prohibition of casino activities in the Republic of Uzbekistan, which is due to the fact that there is no legal regulation of the organization of gambling games (except lotteries), and the illegal organization of gambling games is criminally punishable (Article 278 of the Criminal Code of Uzbekistan), participation in gambling games not permitted by law is an administrative offense (Article 191 of the Criminal Code of Uzbekistan).

b) Realtors must apply CDD measures with respect to both the buyer and the seller (clauses 14-20 of the ICR of 24.08.2011 No. 2257) when establishing a business relationship, conducting one-time transactions exceeding 500 minimum statutory monthly pay (11500 USD), when ML/TF is suspected (regardless of any exclusions and thresholds), when there is doubt about the reliability or sufficiency of previously obtained data. CDD measures must be applied to both the buyer and the seller, as well as to existing customers.

c) Precious metals and stones dealers are required to apply CDD measures (clauses 11 – 17^2 of the ICR of 03.11.2009 No. 2034) when establishing a business relationship, conducting one-time transactions exceeding 600 minimum statutory monthly pay (13800 USD); when ML/TF is suspected (regardless of any exceptions and thresholds), when there is doubt about the reliability or sufficiency of previously obtained data. CDD measures must be applied to both the buyer and the seller, as well as to existing customers.

d) Notaries and lawyers' groups shall apply CDD measures in cases established by R.22 (cl. 2, 16 of the ICR of 19.10.2009 No. 2020). They shall apply CDD measures when establishing a business relationship, conducting one-time transactions exceeding 500 minimum statutory monthly pay (11500 USD); when there is suspicion of ML/TF (regardless of any exceptions and thresholds), when there is doubt about the reliability or sufficiency of previously obtained data. CDD measures must be applied to both the buyer and the seller, as well as to existing customers.

   According to Art. 17 of Law "On Auditing Activity" of 26.05.2000 No. 76-II, auditing organizations can render professional services, including accounting. The law on auditing activity prohibits independent (private) practice of auditors (professional accountants). Audit organizations shall apply CDD measures (clauses 18-28 of the ICR of 15.12.2018 No. 3101) when establishing business relations, one-time transactions exceeding 400 RSV (9200 USD)[130]; when there is suspicion of ML/TF (regardless of any exceptions and thresholds), when there is doubt about the reliability or sufficiency of previously obtained data. CDD measures must be applied to both new and existing customers.

e) The Uzbekistan legislation does not provide for the establishment of establishment of local trusts on the territory of the country, in this regard the activity of providing services related to the registration of trusts is prohibited. The provision of services related to the registration of companies (agent for the creation of legal entities) is not regulated by the AML/CFT/CPF legislation and such persons are not subject to the CDD obligations.

Criterion 22.2

1569. All DNFBPs are required to keep information, CDD materials, and customer identification data for at least 5 years after conducting transactions or terminating a business relationship with customers (Art. 21 of the AML/CFT Law). The corresponding obligations are fully established in the ICR for DNFBPs (audit organizations – cl. 52 of the ICR of 15.12.2018 No. 3101, realtors – cl. 11 of the ICR of 24.08.2011 No. 2257, notaries and lawyers – cl. 11-1 of the ICR of 19.10.2009 No. 2020, lotteries – cl. 44 of the ICR of 17.06.2021 No. 3310, precious metals and stones dealers – cl. 26-3 of the ICR of 03.11.2009 No. 2034). However, there is no requirement to store the results of any analysis performed.

[130]. The RSV size (according to the comments of Uzbekistan and the minimum statutory monthly pay) is 245 000 sums per month (cl. of Presidential Decree of 30.12.2020 No. PP-4938) or 23 USD at the rate of 11.05.2021.

Criterion 22.3

1570. Practically for all DNFBPs ICRs contain requirements to identify and service foreign PEPs, PEPs of an international organization, as well as their relatives and close associates. However, there is a deficiency that controls for identifying and servicing national PEPs have not been established.

Criterion 22.4

1571. All DNFBPs must take measures to prevent the use of technological advances for ML/TF/PF purposes and assess the risks of using new technologies before they are used (lotteries – cl. 6, 31 of the ICR of 17.06.2021 No. 3310, realtors – cl. 20^4 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 17^6 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 23^4 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 34 of the ICR of 15.12.2018 No. 3101).

Criterion 22.5

1572. DNFBPs are not permitted to rely on third parties in conducting CDD.

Weighting and Conclusion

1573. DNFBPs are subject to all requirements of AML/CFT legislation on an equal footing with FIs. There are the following deficiencies: deficiencies in relations with national PEPs, a number of DNFBPs lack the obligation to file an STR when they cannot conduct CDD. Organizations performing the duties of an agent to establish legal entities are not subject to AML/CFT/CPF requirements.

1574. **Recommendation 22 is rated Partially Complaint.**

Recommendation 23 - DNFBPS: other measures

1575. In the 2010 MER, Uzbekistan was rated under R.16 as "NC". The main deficiencies were related to ML/TF criminalization, lack of prohibition and responsibility of DNFBP employees and senior managers for informing customers about filing STRs, lack of requirements for mandatory employee vetting, and mandatory training.

Criterion 23.1

1576. DNFBPs are subject, along with FIs, to requirements to file STRs to a specially authorized state body, including on attempted suspicious transactions, in the prescribed manner no later than one business day following the day of their detection (Art. 15 of the AML/CFT Law).

a) Notary offices and lawyers' groups and auditing companies are reporting entities and must file STRs (Art. 15 of the AML/CFT Law, cl. 26^1, 27-29 of the ICR of 19.10.2009 No. 2020, cl. 40-42 of the ICR of 15.12.2018 No. 3101).

b) Clauses 18, 22 of the ICR of 03.11.2009 No. 2034 contain obligations and criteria for precious metals and stones dealers to file STRs to the authorized body, including a minimum amount of 300 RSV (6900 USD)[131] to be considered a suspicious transaction.

c) The Uzbekistan legislation does not provide for the establishment of trusts on the territory of the country and regulates tax legal relations arising in connection with the participation of residents in unincorporated bodies. Tax legislation of the Republic of Uzbekistan in the framework of intergovernmental cooperation with foreign countries (53 agreements) allows tax control of residents and non-residents of the Republic.

Criterion 23.2

1577. The requirements for internal control of DNFBPs are stipulated by ICRs, which are approved by the supervisory authorities together with the authorized body (Art. 6 of the AML/CFT Law). Besides

[131] The RSV size (according to the comments of Uzbekistan and the minimum statutory monthly pay) is 245 000 sums per month (cl. of Presidential Decree of 30.12.2020 No. PP-4938) or 23 USD at the rate of 11.05.2021.

that, Art. 15 of the AML/CFT Law establishes the obligation for DNFBPs to organize and implement internal control systems (lotteries – cl. 5, 9 of the ICR of 17.06.2021 No. 3310; realtors – cl. 5, 8 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 5, 7 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 6, 9 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 5, 11 of the ICR of 15.12.2018 No. 3101).

1578. DNFBPs are required to:

- designate special officers to carry out activities for AML/CFT purposes (lotteries – cl. 4 of the ICR of 17.06.2021 No. 3310; realtors – cl. 4, 6, 7 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 6 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 5, 7, 8 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 7, 8, 9 of the ICR of 15.12.2018 No. 3101);
- have vetting procedures to ensure high standards of employee qualifications (lotteries – cl. 11 of the ICR of 17.06.2021 No. 3310; realtors – cl. 7 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 6 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 8 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 7, 8, 9 of the ICR of 15.12.2018 No. 3101);
- conduct ongoing training for employees (lotteries – cl. 13 of the ICR of 17.06.2021 No. 3310; realtors – cl. 12 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 10 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 13 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 10 of the ICR of 15.12.2018 No. 3101);
- conduct an independent audit of internal controls (lotteries – cl. 14 of the ICR of 17.06.2021 No. 3310; realtors – cl. 8 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 7 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 9 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 11 of the ICR of 15.12.2018 No. 3101);
- require compliance with AML/CFT measures from their foreign offices (audit organizations – cl. 16-17 of the ICR of 15.12.2018 No. 3101; lotteries – cl. 5-1, 5-2 of the ICR of 05.11.2009 No. 2037).

1579. There are no R.18 requirements for the organization of internal control within financial groups and requirements for foreign units (except for audit organizations and lotteries as to foreign units).

Criterion 23.3

1580. DNFBPs are required to take enhanced CDD measures if one of the parties to the transaction is a person domiciled, resident or registered in a State not participating in international AML/CFT cooperation or in an offshore zone. These persons are categorized as high risk (lotteries – cl. 19, 29 of the ICR of 17.06.2021 No. 3310; realtors – cl. 14, 20^2 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 17^1, 17^4 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 16, 23^2 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 30, 31 of the ICR of 15.12.2018 No. 3101). However, there are shortcomings noted in R.19.

Criterion 23.4

1581. The AML/CFT law ensures confidentiality and restricts access to information. DNFBPs are also prohibited from disclosing the fact that STRs or other information are filed to the FIU (Art. 19, 20 of the AML/CFT Law). The relevant requirements are also set out in the ICR for DNFBPs (lotteries – cl. 47 of the ICR of 17.06.2021 No. 3310; realtors – cl. 29 of the ICR of 24.08.2011 No. 2257; precious metals and stones dealers – cl. 26 of the ICR of 03.11.2009 No. 2034; notary offices and lawyers' groups – cl. 33 of the ICR of 19.10.2009 No. 2020; audit organizations – cl. 56 of the ICR of 15.12.2018 No. 3101). As applied to notary offices and lawyers' groups and auditing organizations, the law does not impose any additional conditions relating to the requirements of R.21 to the extent that attempting to dissuade a customer from involving in illegal activities does not constitute disclosure.

Weighting and Conclusion

1582. The requirements of R.23 are fulfilled to a partial extent, the obligation to file STRs applies to all categories of DNFBPs. There are deficiencies related to implementing the R.18 requirements, some deficiencies under R.21 (notary offices and lawyers' groups).

1583. **Recommendation 23 is rated Largely Compliant.**

Recommendation 24 - Transparency and beneficial ownership of legal persons

1584. In the 2010 MER, Uzbekistan was rated "PC" on R.33 due to the lack of legislative measures to establish and verify beneficial ownership information of legal persons. Besides, the legal person registration system was not used for AML/CFT purposes. These deficiencies were addressed following the review of the 4th follow-up report in 2015.

Criterion 24.1

1585. The Republic of Uzbekistan has mechanisms that allow to identify legal persons and describe the nature of their activities. Chapter 4 of the Civil Code No. 163-I of 21.12.1995 (Art. 39, 40) regulates the concept, forms and main characteristics of legal persons, and also establishes the procedures for creation, as well as requirements and conditions for state registration.

1586. The procedure and terms of state registration of natural and legal persons that are business entities, as well as the list of information required for registration are defined in the Regulation on the procedure of state registration of business entities (approved by Resolution of the CM of 09.02.2017 No. 66).

1587. When applying for registration, legal entities must provide details of their founders (Annex No. 5 to Regulation on the procedure of state registration of business entities). Besides, since April 2021, all applicants must provide their BO information at registration by entering it into the questionnaire and update this data (changes to the state registration procedure approved by Resolution of the CM of 02.12.2020 No. 763).

1588. In the Republic of Uzbekistan there is a Single State Register of Business Entities (hereinafter – SSRBE)[132], which contains basic information on the creation, reorganization, and liquidation of legal persons and other business entities. The information and documents contained in the Register are open and accessible to any interested person, except for the information to which access is restricted by law. The Register is formed and maintained by PSA and is updated on a daily basis.

1589. The minimum amount of information placed and regularly updated in the Registry includes TIN, information on the body that carried out the registration, date and number of registration, name of the legal entity and its legal form, current status (active, liquidated or in the process of liquidation), size of the charter fund, information on the founders and their shares in the charter fund (even if there are several founders), contact information (e-mail address, phone number, address), and information on the head (full name and TIN).

1590. According to Decree of the President of the Republic of Uzbekistan UP-6191 of 23.03.2021, from June 1, 2021 law enforcement agencies as well as a number of other competent state bodies are provided with unimpeded access to information from automated systems of state registration and registration of business entities.

1591. Provision of documents from the Register, including in electronic form, is carried out on a fee basis, except for their provision at the request of state bodies and the business entity itself (Chapter 4 of Regulation "On the procedure of maintenance of the Single State Register of Business Entities" approved by Resolution of the CM of February 9, 2017. No. 66).

[132] https://fo.birdarcha.uz/pub/search; https://stat.uz/ru/uslugi-1/svedeniya-iz-egrpo

Criterion 24.2

1592. In 2019, the Republic of Uzbekistan approved a national ML/TF risk assessment report, which covers all categories of legal persons created in the country Competent authorities have generally demonstrated a good understanding of the vulnerabilities of legal persons. At the same time, the degree of understanding among government agencies varies.

Criterion 24.3

1593. PSC enter information into the Register on the basis of documents submitted during state registration, as well as upon submission of information and (or) documents by state bodies and other organizations (clauses 3, 7 of Annex No. 2 of Resolution of the CM of 09 February 2017 No. 66.). The information in the Register must contain (cl. 5 of Annex No. 2 to Resolution of the CM of 09.02.2017 No. 66) company name, number of state registration certificate and registration date, legal form and form of ownership, founders, information about the head, including full name and TIN, information on the regulatory powers, as well as postal address (cl. 13 of Annex No. 2 to Resolution of the CM of 09.02.2017 No. 66). The SSRBE does not contain information on directors of a legal person.

Criterion 24.4

1594. The charter of a limited and additional liability company must contain information on the size and nominal value of the share of each participant in the company (Art. 13 of Law of 06.12.2001 No. -310-II). The company shall keep documents (including the charter) at the location of its executive body or in any other place known and accessible to the company participants (Art. 48 of Law of 06.12.2001 No.-310-II). When registering all types of legal persons created in Uzbekistan, provide to PSC the information specified in the analysis of criterion 24.3. The founding agreement determines the composition of the founders (participants) of a company (Art. 12 of Law of 06.12.2001 No-310-II). The requirements to the founding agreement are the same for all LLCs.

1595. A joint-stock company is a commercial organization whose charter fund (charter capital) is divided into a certain number of shares certifying the rights of the shareholders in relation to the company (Art. 3 of Law "On Joint-Stock Companies and Protection of Shareholder Rights" No. 370 of 06.05.2014). The register of shareholders of a company shall be formed by the Central Securities Depository, which performs the functions of the central registrar, according to the status of depo accounts of securities holders (Part 2 Art. 42 of Law of 06.05.2014 No. 370). The register is a list of registered holders of shares formed as of a certain date, indicating their name, number, nominal value and type of shares held by them, as well as data which allows information to be sent to persons registered in the register (Art. 42 of the Law of 06.05.2014 No. 370).

Criterion 24.5

1596. The Republic of Uzbekistan has mechanisms for timely recording of relevant information on legal persons and its updating. The SSRBE is maintained centrally in electronic form through an automated system of state registration and registration of business entities according to the form established by the MJ (cl. 6 of Annex No. 2 to Resolution of the CM of 09.02.2017 No. 66). In case of discrepancies between the information in the constituent documents contained in the electronic file of the SSRBE and the founding documents held by the business entity, the founding documents contained in the electronic file of the Register shall prevail (cl. 8 of Annex No. 2 to Resolution of the CM of 09.02.2017 No. 66).

1597. Due to the priority of information contained in the Register, it is relevant and accurate, which in turn contributes to the fact that legal entities keep their information in the Register up to date. Uzbekistan's legislation provides for administrative liability for violation of the terms and procedure for informing the registration bodies about changes in the registration documents of legal entities (Article 176-2 of the CAO). Legal persons shall inform state authorities about changes in charter documents, founders and composition of their shares, beneficiaries, as well as all other updates within 30 days from the date of such changes. 30 days is the maximum period. As a rule, it happens within 10 days.

1598. There are no sanctions for providing inaccurate information at the registration stage. Nevertheless, assessors believe that checks by the competent authorities after registration, allow to identify mistakes in the registration data, and thus prevent the provision of inaccurate information.

Criterion 24.6

1599. Competent authorities rely on a variety of available sources of information to obtain BO data on legal persons, in particular information collected by FIs and DNFBPs in applying CDD measures, data from the SSRBE, information held by competent authorities in other countries in relation to the legal person and open data sources. When applying for registration of legal entities applicants must submit detailed information on the founders and BO (Annex No. 5 to the Regulation on state registration of business entities). A deficiency under criterion 24.3 of the lack of information about the legal person's directors in the SSRBE also applies to the fulfillment of this criterion.

Criterion 24.7

1600. Applicants must provide details of the founders and BO when applying to the registration authority (Annex No. 5 to the Regulation on state registration of business entities). See also Criterion 24.1. The definition of BO is given in the ISR for FIs (approved by Decision of the Board of CB and DCEC No. 343-B and 14 of 17.04.2017) and is consistent with the definition in the FATF Glossary. A BO is a natural person who ultimately owns or actually controls a customer, including a legal person, for whose benefit a transaction in cash or other property is conducted. The definition of BO in the ICR of other reporting entities is similar to that of banks. To identify a BO, the ownership and management structure is examined on the basis of the founding documents defined by law (the charter and (or) the foundation agreement, regulation.

1601. FIs and DNFBPs are required to conduct identification procedures and CDD measures, including verification and regular updates of customer and BO information (Art. 15 of the AML/CFT Law). The obligation to update CDD information is set out in the ICR for FIs and DNFBPs (see sub-criterion 10.7b, sub-criterion 22.1). According to the analysis of compliance with the requirements of sub-criterion 10.7b, insurance companies do not have specifics about updating information obtained as a result of CDD measures for high-risk customers. See also Criterion 24.6 analysis. The country has created conditions to ensure the accuracy and relevance of information on the BO to the extent possible.

Criterion 24.8

1602. In accordance with Part 1 of Art. 201 of the CPC of September 22, 1994 heads and other officials of enterprises, institutions and organizations are obliged, upon request of an inquirer, investigator, prosecutor or court, to provide documents in their possession or specially drawn up on the basis of information available to them.

1603. DNFBPs are obliged to identify the customer's BO and provide information upon written request to the DCEC. Also, in accordance with Part 1 of Art. 201 of the CPC of September 22, 1994, heads and other officials of enterprises, institutions and organizations are obliged, upon request of an inquirer, investigator, prosecutor or court, to provide documents in their possession or specially drawn up on the basis of information available to them.

1604. FIs are obliged to identify the customer's BO and provide information upon written request to the DCEC. Also, in accordance with Part 1 of Art. 201 of the CPC of September 22, 1994 heads and other officials of enterprises, institutions and organizations are obliged, upon request of an inquirer, investigator, prosecutor or court, to provide documents in their possession or specially drawn up on the basis of information available to them.

Criterion 24.9

1605. FIs and DNFBPs must keep information on transactions in monetary funds or other assets, as well as CDD identification and materials for the periods prescribed by law, but not less than five years after such transactions or termination of the business relationship with customers (Art. 21 of the AML/CFT law). When companies are liquidated, their archives must be transferred to the appropriate state or

non-state archives in accordance with the procedure established by law (Art. 5 No. LRU-252 of 15.06.2010).

1606. Data contained in the Registry is stored on a permanent basis according to the principle of "accumulation". Even after the termination of the business entity (liquidation, bankruptcy), the data is not deleted and is stored on the PSA servers (Resolution of the CM of 09.02.2017 No. 66).

Criterion 24.10

1607. Written orders and resolutions of an investigator, issued in accordance with the law on the cases before him/her, are binding on all enterprises, institutions, organizations, officials and citizens (Part 4 of Art. 36 of the CPC). The DCEC is also entitled to file written requests to organizations for additional information and duly certified copies of documents related to a particular transaction, if there is a need to verify the reliability of obtained information, if there is information about the possible conducting of such transaction for ML/TF purposes, as well as in the framework of the obligations under international treaties of the Republic of Uzbekistan in the AML/CFT field (cl. 17-20 of Annex 1 to the Resolution of the CM of 29.06.2021 No. 402 “Regulations on the provision of information related to AML/CFT/CPF”).

1608. Competent authorities have unrestricted access to the adequate, accurate and current basic and beneficial ownership information on all types of legal persons created in the country, in a timely manner. The source of this information is SSRBE, data collected by the FIs and DNFBPs and available on the website of other state authorities.

Criterion 24.11

1609. In Uzbekistan the issue of bearer shares and bearer warrants is impossible. A share is a registered issuable security (Art. 3 of Law of 03.06.2015 No. LRU-387). The issue and circulation of bearer securities was possible under the wording of the Law "On the Securities Market" dated July 22, 2008, No. LRU-163. However, after the release of No. LRU-223 of 22.09.2009 on amendments and additions to certain legislative acts in connection with the improvement of AML/CFT legislation, these provisions became no longer in force.

Criterion 24.12

1610. The concept of "nominee director" does not exist in the legislation of the Republic of Uzbekistan. The issue of nominee shares in Uzbekistan is also not possible. At the same time, there is an institution of entrusted management in Uzbekistan. See in the analysis on Recommendation 25.

Criterion 24.13

1611. Uzbekistan’s legislation does not explicitly penalize the failure to provide data on legal persons and BO. Sanctions are applied for failure to provide information about changes in registration data of legal persons or submission of false information about changes in address, bank details or re-registration of a business entity. This entails a fine of ten to fifteen RSV for officials (Article 176-2 of the CAO).

1612. All enterprises, institutions, organizations, officials and citizens are obliged to comply with the written orders and resolutions of the investigator issued in accordance with the legislation on the case under investigation. For non-compliance with the above requirements, individuals are sanctioned on the basis of the CAO (Art. 176 note 2, 194, 197, 198). Besides this, for doing business without state registration the maximum penalty is a fine of 5 to 15 RSV (Art. 176 of the CAO). The amount of sanctions, given the average wage in the country, according to the competent authorities, is proportionate and dissuasive. Assessors agree when it comes to bona fide individuals, but these sanctions may not have the desired effect when applied to non-bona fide individuals.

1613. Uzbekistan applies the practice of preventing violations of the law by legal persons, which consists in rejecting applications from this category of persons in case of their improper execution. Thus, between 2016 and 2020, state registration and re-registration of business entities was denied in 8017 cases. At the same time, taking into consideration the limited number of sanctions against persons for

failure to provide information on legal entities and BO, assessors consider the sanctions applied by the country to be not sufficiently dissuasive and proportionate.

Criterion 24.14

1614. The SSRBE is a publicly available source of basic information about legal persons, which may be used by foreign competent authorities. The country does not provide information on what legal acts regulate the exchange of information on shareholders. The legislation of Uzbekistan allows investigations at the request of the competent authorities of a foreign country, as well as the transfer and exchange of information received in the framework of other forms of international cooperation. Such norms are contained, among others, in Article 15 of the Law of the Republic of Uzbekistan of 25.12.2012 No. LRU-344 "On Criminal Intelligence and Detective Operations" and Article 45 of Law of the Republic of Uzbekistan on 16.09.2016 No. LRU-407 "On Internal Affairs Bodies". See also criterion 40.9.

Criterion 24.15

1615. No legal provisions prevent the DCEC from providing its partners with feedback, upon request or when possible, on their use of the information provided and on the results of the analysis based on the information provided. According to cl. 2 of Presidential Decree of 23.05.2018 No. 5446, cooperation and information sharing with competent authorities of foreign countries, international specialized and other organizations on the fight against economic crimes and corruption, as well as AML/CFT/CPF, is one of the priority tasks of the DCEC. See also Criterion 40.10. At the same time, the assessed country did not provide information on the requirement or prohibition to provide feedback by other competent authorities.

Weighting and Conclusion

1616. A legal framework for various organizational and legal forms of legal persons has been established in Uzbekistan. Legal persons undergo the procedure of state registration, and basic information about them is recorded in the SSRBE, some of this information is publicly available. The NRA covers all categories of legal persons created in Uzbekistan.

1617. Liability and sanctions cover only a small portion of possible violations and are not considered by assessors to be proportionate and dissuasive.

1618. **Recommendation 24 is rated Largely Compliant.**

Recommendation 25 - Transparency and beneficial ownership of legal arrangements

1619. In the 2010 MER, Uzbekistan was rated under R.34 as "NA" due to the fact that the legal system did not provide for the establishment of trusts and the legal concept of trusts did not exist.

1620. Legal arrangements in the sense in which these terms are used in the FATF Recommendations cannot be established in Uzbekistan. The Republic of Uzbekistan is not a party to the 1985 Hague Convention on the Law Applicable to Trusts and their Recognition. However, the law provides for legal relationships between foreign trusts and residents to generate income for the benefit of the settlor. The settlor of a foreign trust is registered with the tax authorities and informs the Tax committee of his participation in the trust relationship (Art. 22 and 209 of the TC). There are no obstacles to obtaining information from a resident participating in a foreign trust. The concept of "trust" was introduced in the national legislation with the adoption of the new version of the TC, which entered into force on January 1, 2020. In accordance with Article 35 of the TC, trusts are referred to foreign bodies established in accordance with the legislation of a foreign State and having the right to carry out activities aimed at generating income in the interests of its participants (shareholders, settlors or other persons) or other beneficiaries.

1621. Uzbekistan has a "fiduciary management" institution, which differs from trusts established in countries with non-continental legal systems. The basis for the establishment of entrusted management of property in Uzbekistan is an agreement concluded between the settlor and entrusted manager (Art. 850 of the Civil Code). The objects of fiduciary management may be enterprises and

other property complexes, separate objects relating to immovable property, securities, exclusive rights and other property. Money cannot be an independent object of fiduciary management (Art. 851 of the Civil Code). The settlor of the fiduciary management of the property is the owner of the property. The fiduciary manager may be a citizen or a legal person. Any person may be a beneficiary, except for the fiduciary manager (Art. 852 of the Civil Code). Under the contract, the settlor transfers the property to the fiduciary manager for a fixed term for fiduciary management, and the manager is obliged to manage this property for the benefit of the settlor or the person indicated by him (the beneficiary). The transfer of property into fiduciary management does not entail the transfer of ownership rights to the fiduciary manager. In carrying out fiduciary management of property, the fiduciary manager has the right to make with respect to this property according to the contract of fiduciary management any legal and actual actions in the interests of the settlor or the beneficiary (Art. 849 of the Civil Code).

1622. Transactions with the property entrusted into fiduciary management are carried out by the fiduciary manager in his own name, indicating that he acts in his capacity as such a manager. This condition is deemed to be met if the other party is informed that the manager is acting in this capacity, and a note is made in the written documents after the name or the name of the manager. In the absence of any indication that the fiduciary manager is acting in this capacity, the manager is obliged to the third parties personally and is liable to them only with the property belonging to him (Art. 849 of the Civil Code). The property transferred into fiduciary management is segregated from other property of the settlor and the fiduciary manager. This property is reflected by the fiduciary manager on a separate balance sheet and there is an independent accounting for it. A separate bank account is opened for settlements on activities related to fiduciary management (Art. 855 of the Civil Code).

1623. The fiduciary property management contract is concluded in written form and must include information on the beneficiary; about the person receiving the property in case of termination of fiduciary management[133]; terms of submission of reports by the manager to the settlor and the beneficiary; the amount and form of remuneration of the manager (if stipulated by the contract). The transfer of immovable property for fiduciary management is subject to state registration in the same manner as the transfer of the property ownership (Art. 854 Civil Code).

Criterion 25.1

1624. The requirements of sub-criteria **a)** and **b)** are not applicable to the Republic of Uzbekistan due to the fact that the legislation does not provide for the establishment of trusts on its territory.

1625. There is an institution of "entrusted management" in the Republic of Uzbekistan. However, there are no directly applicable rules in the legislation providing for the obligations of entrusted managers to keep sufficient and accurate information about the identity of the settlor or any other individual exercising ultimate actual control. At the same time, Art. 853 of the Civil Code establishes that the contract of entrusted management must contain information about the beneficiary. At the same time, it is not specified what kind of information is referred to and to what extent this information must be complete, accurate and up-to-date.

1626. According to Art. 22 of the TC, taxpayers are obliged to keep tax returns and other documents necessary to calculate and pay taxes for five (5) years.

1627. FIs and DNFBPs will apply CDD measures when accepting a resident who applies to carry out a transaction in respect of a party to a foreign trust. It should also be noted that according to paragraph 29-1 of the ICR for banks (No. 2886 of May 23, 2017), foreign entities are subject to requirements similar to those established for legal persons. Similar requirements are established for NBCIs (cl. 28-1 of the ICR for NBCIs No. 2925 of 04.09.2017). See also the analysis on Recommendation 10.

[133] At the termination of the entrusted management contract, the property held in entrusted management shall be transferred to the settlor, unless the contract stipulates otherwise.

Criterion 25.2

1628. Application of this criterion is possible only when residents apply for services to FIs and DNFBPs in order to carry out a transaction in respect of a party to a foreign trust. In this case, reporting entities must conduct CDD when establishing a business relationship with their customers. See also the analysis of criterion 25.1.

Criterion 25.3

1629. Accounts in national and (or) foreign currency in commercial banks of the Republic of Uzbekistan shall be opened for persons who applied for banking services in accordance with the procedure specified in cl. 16 and 21 of the "Instruction on bank accounts opened with the banks of the Republic of Uzbekistan" (Reg. No. 1948 of April 27, 2009) (Instruction-1948).

1630. When opening bank accounts, applicants must undergo the CDD procedure regulated by cl. 22-47 of "ICR on AML/CFT/CPF in commercial banks" (Reg. No. 2886 of 23.05.2017) (ICR-2886). When conducting CDD of legal persons, a bank must identify the BO who ultimately owns or controls the customer, apply measures to verify the BO's identity using information obtained from a reliable source, including by examination of:

- the ownership and management structure of the customer;
- founders of the customer (shareholders/participants owning at least ten percent of the company's shares/interests);
- personal data of a natural person (persons) who ultimately owns a share (at least ten percent) of the legal person (if any);
- if doubts arise as a result of the measures taken as to whether the person (persons) having the controlling interest, is BO, or in the absence of persons managing the ownership of shares and personal data of the natural person (persons) exercising control over the legal person, other methods (if any) are used).

1631. If BO cannot be identified, commercial banks must identify the person in a senior management position and take reasonable steps to verify his or her identity.

1632. It should be noted that clause 23 of ICR-2886 and cl. 81 of Instruction of the MJ No. 1948 established that if there is no possibility to conduct CDD, a commercial bank must inform the FIU and refuse to open an account. Besides that, the legislation does not allow remote opening of accounts for customers whose founders are non-residents of the Republic of Uzbekistan (cl. 231 of ICR-2886 and clause 82 of Instruction-1948). See also the analysis on criterion 25.1 with respect to measures applied by FIs and DNFBPs when accepting a resident who applies for the purpose of carrying out a transaction in respect of a party to a foreign trust.

1633. According to Art. 850 of the Civil Code entrusted manager when dealing with property placed into entrusted management indicates that he acts as such a manager.

Criterion 25.4

1634. Uzbekistan’s legislation does not prevent legal persons, regardless of their structure and model, from providing information to competent authorities or FIs and DNFBPs upon request.

Criterion 25.5

1635. LEAs are granted with full powers to request and receive any information from legal legal arrangements within their competence. The scope of LEAs’ powers, reflected in the analysis on the requirements of Recommendation 31, may be used by them to obtain the information necessary to meet this criterion.

1636. According to Art. 26 of the TC, the tax authorities have the right to require taxpayers and third parties to submit documents and data (information), including in electronic form, necessary for the calculation and payment of taxes and fees; to seize documents and electronic media related to the calculation of taxes and fees; to take photographs and video recordings, to receive explanations and other information.

Criterion 25.6

1637. There are no special norms for international cooperation in relation to trusts in Uzbekistan. At the same time, according to the legislation there are no obstacles to the exchange of information between the competent authorities of Uzbekistan and foreign partners in the framework of international cooperation. According to cl. 2 of Presidential Decree of 23.05.2018 No. 5446, interaction and data sharing with the competent authorities of foreign states, international and other organizations on the fight against economic crimes and corruption, as well as AML/CFT/CPF is one of the priority tasks of the DCEC.

Criterion 25.7

1638. Trusts cannot be established in Uzbekistan. The legislation provides liability for entrepreneurial activity without state registration (Art. 188 of the CC). If residents apply for services to FIs or DNFBPs, the responsibility for fulfilling the requirements of the relevant AML/CFT law, including the collection of the customer and BO information will lie on reporting entities. If FIs or DNFBPs are unable to conduct CDD due to a lack of required information, they can refuse service to the the customer. Violation of AML/CFT/CPF laws by reporting entities is also punishable by a fine of fifteen to thirty RSV (Art. 179, note 3 of the CAO).

Criterion 25.8

1639. Trusts cannot be established in Uzbekistan. There are no obstacles to obtaining information from a resident participating in a foreign trust.

Weighting and Conclusion

1640. Trusts cannot be established in the Republic of Uzbekistan, in this connection a number of criteria of the recommendation are not applicable. Measures envisaged by the current legislation in relation to foreign trusts, in particular those connected with keeping information about the beneficiary, as well as the requirements for CDD measures (except for banks), seem insufficient.

1641. **Recommendation 25 is rated Partially Compliant.**

Recommendation 26 - Regulation and supervision of financial institutions

1642. In the 2010 MER, Uzbekistan was rated under R.23 as "PC". The legal framework in the field of supervision and monitoring for AML/CFT purposes was not clearly regulated in sectoral laws, there was no information on the application in the banking, insurance and securities sector of the Basic Principles for AML/CFT purposes, market entry procedures are detailed only in relation to the banking sector, there was no authority for supervision and monitoring in the Law on leasing.

Criterion 26.1

1643. Uzbekistan has designated AML/CFT regulatory and supervisory authorities for all types of FIs: banks, NBCIs, payment institutions, payment system operators, electronic money system operators - the Central Bank; insurance companies, insurance brokers, professional securities market participants and leasing organisations - the Ministry of Finance and the FIU; postal service operators and providers - the State Inspectorate for Control in the Field of Information and Telecommunications of the Republic of Uzbekistan; commodity exchanges - the Antimonopoly Committee; exchange members - the exchanges themselves and FIU.

Criterion 26.2

1644. Most FIs are licensed: Banks (Art. 15 of Law No. ZRU-580 of 05.11.2019), NBCIs (Art. 9 of Law No. 3RU-53 of 20.09.2006, cl. 1-2 of Resolution of the Central Bank Board of 10.12.2003 No. 1291), insurance companies (Art. 6 of Law of 05.04.2002 No. 358-II), professional participants in the securities market (cl. 2 of Resolution of the Cabinet of Ministers of 09.06.2003 No. 308), exchange members (Art. 3 of Law of 12.09.2014 No. ZRU-375), payment organizations, payment system operators (Art. 12 of Law No. ZRU-582 of 11.11.2019). The operator of the electronic money system

is the bank which ensures the operation of the electronic money system and/or the payment organization which has the relevant licence (paragraph 3 of the Rules on Electronic Money Issue and Circulation in the Republic of Uzbekistan, 29.04.2020 No. 3231). Insurance agents are insurance intermediaries, but their activities are not licensed or subject to AML/CFT supervision. According to Order No. 1213 of the Minister of Finance of 01.02.2003, insurance agents work for and on behalf of insurance organisations (insurers) on the basis of contracts of mandate (agency agreements).

1645. Leasing companies, mobile phone operators that carry out money transfers, and postal service providers are not subject to licensing/registration. There is one state postal operator in the country on the basis of the Decree of the President of the Republic of Uzbekistan "On measures aimed at reorganizing and improving the management of information systems sphere" No. UP-1823 of July 23, 1997.

1646. There is no direct requirement to prohibit the opening of shell banks in the legislation, but at the same time the norms defining the procedure for opening banks or representative offices actually do not allow opening a bank that does not have a physical presence in the country. The establishment by foreign banks of branches in the Republic of Uzbekistan is not allowed (Art. 30 of Law of 05.11.2019 No. ZRU-580).

Criterion 26.3

1647. The requirements of this Criterion are implemented to a certain extent for banks and NBCIs (Art. 24, 36 of Law of 25.04.1996 No. 216-I, Art. 61 of Law of 21.12.1995 No. 154-I, cl. 7 of Resolution of the Board of the Central Bank of 13.04.2010, No. 2093, cl. 10 of Resolution of the Board of the Central Bank of 10.12.2003 No. 1291). The founders and shareholders of a bank or non-banking credit organization shall be considered non-compliant with the requirements for business reputation in limited cases when they do not have a criminal record only for economic and administrative offences (not for all categories of crime). For other FIs there are no requirements. The requirements do not apply to persons associated (affiliated) with the beneficial owners and senior managers of FIs.

Criterion 26.4

a) Regulation and supervision of banking activities are in line with the core principles. Supervision by the Central Bank and the Ministry of Finance (as far as insurance companies are concerned) for AML/CFT purposes is applicable to the consolidated group. There is no information about the organization of consolidated supervision of professional participants in the securities market.

b) Risk-based supervision for NBCIs, sector of payment organisations is established by the CB (see criterion 26.5). Postal operators are reporting entities in the AML/CFT field for relevant competent authorities (Mininfocom and Uzkomnozorat); exchange members are reporting entities in this field for two commodity exchanges – UZEX and RUACE. Monitoring and supervision have been established, but the risk-based approach has not been implemented.

Criterion 26.5

1648. The frequency and intensity of remote AML/CFT supervision of banks, NBCIs and the payment institution sector is based on the RBA, which consists of enhanced and standard monitoring:

a) The monitoring programme (a set of monitoring tools) for remote AML/CFT supervision for banks is developed by the CB based on a system of indicators that include indicators on the bank's customers, operations, products and services, their risks, as well as indicators designed to assess the effectiveness of AML/CFT internal controls. The indicators are taken from the reporting system, which consists of occasional, monthly, quarterly and annual reports (Chapter 4, paragraphs 35-36 of the Methodology approved on 06.11.2019 by the Deputy Chairman of the Central Bank Board).

b) The remote AML/CFT supervision of banks is based on indicator monitoring, based on the ML/TF risks present in the country (SRAs and NRAs) (paragraphs 32, 37 of the Methodology).

c) The standard monitoring programme (set of monitoring tools) is uniform and permanent for all banks (paragraph 38). The enhanced monitoring programme shall be developed for each bank separately,

taking into account the results of standard monitoring, on-site inspections, and other factors affecting the bank's risk profile (paragraph 39).

1649. Similarly, AML/CFT monitoring programmes are developed for the NBCIs and the payment institution sector. The Ministry of Finance has adopted Recommendations on the Application of a Risk-Based Approach (RBA) in the Monitoring and Control of AML/CFT Compliance of Insurance and Leasing companies, which contain certain elements of the RBA, for the insurance and leasing sectors. For the exchange trading sector, the postal operator AML/CFT supervision is present, but without ranking of FIs by risk levels. For the securities sector there is no risk-based AML/CFT supervision.

Criterion 26.6

1650. Authorities involved in monitoring and supervising compliance with ICR on AML/CFT are required to systematically, at least once a year, conduct research, analysis and identification of possible ML/TF/PF risks in their activities, document the results of the research and take appropriate measures to mitigate the identified risks (Art. 71 of the AML/CFT Law). It is not established that an annual ML/TF/PF risk assessment is conducted in relation to FIs and their operations (except Antimonopoly Committee – cl. 25-1 of the ICR of 06.11.2009 No. 2038).

Weighting and Conclusion

1651. Uzbekistan has designated AML/CFT regulatory and supervisory authorities for all types of FIs, most of which are licensed.

1652. The following major deficiencies were identified: for FIs (except banks and NBCIs) there are no requirements to business reputation of beneficial owners, founders and senior managers; business reputation requirements do not apply to persons associated (affiliated) with the beneficial owners and senior managers of all FIs; founders and shareholders of a bank, a microcredit organization are considered non-compliant in limited cases (not for all types of offences); no information on consolidated supervision organization in the securities sector; no risk-based AML/CFT supervision (except CB), and no connection of annual ML/TF/PF risk assessment with the activities of FIs (except for banks, payment institutions, NBCIs).

1653. Insurance agents, postal operators and providers, mobile money transfer operators, leasing organisations are not subject to licensing and/or registration. However, this deficiency is moderate due to the weight of these sectors in financial system.

1654. **Recommendation 26 is rated Partially Compliant.**

Recommendation 27 – Powers of supervisors

1655. In the 2010 MER, Uzbekistan was rated under R.29 as "PC" because only the Central Bank had the ability to impose a broad range of sanctions on reporting financial institutions.

Criterion 27.1

1656. For all categories of FIs, AML/CFT supervision bodies are identified (see Criterion 26.1). These bodies have the appropriate authority (CB – Art. 12, 61, 64 of Law of 11.11.2019 No. ZRU-582; Insurance Market Development Agency under the Finance Ministry – cl. 9 of Regulation approved by Resolution of the Cabinet of Ministers of 31.12.2019 No. 1060; State Inspectorate for Control in the Field of Information and Telecommunications – cl. 10 of Regulation approved by Presidential Decree of 21.11.2018 No. PP-4024; Ministry of Finance –cl.9 sub-paragraph 15 of the Regulation approved by Presidential Decree No. PP-2847 of 18.03.2017). The supervisory body for exchange is the Antimonopoly Committee (see Criterion 26.1), but in turn the two commodity exchanges established in the country – UZEX and RUACE – have the authority to supervise or monitor and ensure compliance of exchange members with AML/CFT requirements. In addition, the specially authorised state body in the field of AML/CFT/PF - the DCEC has the authority to monitor the organisations' compliance with the ICR without interfering with their business activities.

Criterion 27.2

1657. Supervisory authorities for most FIs have the authority to conduct "inspections". The Central Bank (Art. 61, 64 of Law of 11.11.2019 No. ZRU-582), the Insurance Market Development Agency under the Finance Ministry (Art. 10 of Law of 05.04.2002 No. 358-II), the State Inspection for Information and Telecommunications Control (cl. 10 of Regulation approved by Presidential Decree of 21.11.2018 No. 4024). Until 01.05.2021 the Capital Market Development Agency (cl. 12 of Regulation approved by Resolution of the Cabinet of Ministers of 07.08.2019 No. 650, from 01.05.2021 Ministry of Finance monitors compliance with legislation on the securities market, on joint stock companies and on the protection of shareholders' rights (without specifying the power to carry out inspections) – cl. 9 sub-paragraph 16 of the Regulation on the Ministry of Finance, approved by Presidential Decree No. PP-2847 of 18.03.2017 (Annex No. 7)). Supervisory authorities for exchange members - commodity exchanges do not have the power to conduct inspections. At the same time, cl. 9, 10 of Annex No. 3 to Resolution No. 402 of the CM of 29.06.2021 established that all authorised supervisory bodies other than the CB, can conduct inspections of organisations conducting transactions with cash or other property on AML/CFT/CPF issues. All supervisory bodies are entrusted with AML/CFT/CPF tasks (taking into account the amendments and additions made to the relevant regulations of ministries and agencies by Presidential Decree No. UP-6252 of 28.06.2021. However, according to paragraph 1 of Annex No. 3 to this Resolution, the requirements of Regulation in terms of inspections do not apply to inspections conducted by the CB in this area. The CB has developed and approved the Methodological Recommendations on conducting on-site inspections in commercial banks (dated 17.08.2020), non-bank credit institutions (dated 04.09.2020), payment system operators, electronic money system operators, payment institutions (dated 03.02.2021) on AML/CFT/CPF issues.

Criterion 27.3

1658. The CB has the authority to request and inspect reports and other documents and to request clarification of information (Art. 61 of Law of 11.11.2019 No. ZRU-582). The Insurance Market Development Agency under the Finance Ministry has the authority to obtain documents and explanations on issues related to the activities of inspected insurance companies (cl. 9 of Regulation approved by Resolution of the Cabinet of Ministers of 31.12.2019 No. 1060).

1659. The State Inspectorate for Control in the Field of Information and Telecommunications has the right to request and receive necessary information, documents, references and other materials from organizations and agencies (cl. 14(4) of Regulation approved by the Presidential Decree of 21.11.2018 No. 4024), but the range of such organizations is not specified. The Agency for Capital Market Development had similar powers until 01.05.2021 (cl. 12 of Regulation approved by Resolution of the Cabinet of Ministers of 07.08.2019 No. 650) in relation to "state administration bodies, local state authorities, economic management bodies, enterprises, organizations and other legal entities". From 01.05.2021, the Ministry of Finance has no such authority over securities market participants (clause 9, sub-clause 16 of the Regulation on the Ministry of Finance, approved by Presidential Decree No. PP-2847 of 18.03.2017 (Annex No. 7).

1660. JSC " UZEX " has the authority "to request from the members of the exchange information related to the internal control execution" (cl. 268 Rules of exchange trading of UZEX approved by the minutes of the meeting of the Supervisory Board of UZEX of 19.07.2019). Cl. 355 of the Rules of Stock Exchange Trading at RUACE, approved by the Exchange Council - Minutes of 11.08.2015).

1661. It should be noted that practically in all sectors (except banks) the authority to request information from reporting entities does not have AML/CFT specifics. The Finance However, this disadvantage is minor because although there is no explicit requirement to request information specifically for AML/CFT purposes, the wording "to request information within the scope of legislation" covers AML/CFT legislation as well. Ministry is entitled to receive information from leasing entities for risk assessment but it doesn’t include receiving information during the laws observance monitoring. The supervisor of insurance companies has no authority to request any information other than that requested during inspections.

Criterion 27.4

1662. The CB has the power to impose sanctions for violations of AML/CFT/CPF legislation on banks and NBCIs, including orders to eliminate deficiencies, fines of up to 1% of the minimum charter capital, requirements to replace the head and employees of the internal control service, limitation and revocation of the license (cl. 2, 3 of Regulation of 13.01.2010 No. 2063).

1663. The Insurance Market Development Agency under the Finance Ministry can only impose a fine in the amount of 0,05% of the minimum amount of authorized capital established for the insurer in accordance with the legislation on insurance activity (cl. 17-1 of Regulation of 15.08.2008 No. 1842), which is not sufficient to meet the requirements of the Criterion.

1664. Until 01.05.2021 DCMD had the right to suspend some operations of a professional participant, to suspend or terminate the validity of the qualification certificates of securities market experts, to impose fines "as provided by the legislation", to apply to courts "for suspension, termination or cancellation of licenses" (cl. 12 of Regulation approved by Resolution of the Cabinet of Ministers of 07.08.2019 No. 650), but these sanctions do not affect violations in the field of AML/CFT. From 01.05.2021 Ministry of Finance: apply measures and sanctions in accordance with the legislation, in case of detecting violations of AML/CFT legislation (cl. 9 sub-paragraph 15 of Annex 7 of Presidential Decision No. PP-2847 of 18.03.2017).

1665. In accordance with subclause 5 of clause 14 of Regulation on the State Inspectorate for Control in the Field of Information and Telecommunications of the Republic of Uzbekistan approved by Presidential Decree of 21.11.2018 No. PP-4024, the State Inspectorate is entitled to draw up protocols and consider cases of administrative offenses in the field of communication, information, telecommunications technology, use of the radio frequency spectrum and distribution of periodicals, and upon establishing cases of violation by operators and postal service providers of AML/CFT legislation, file materials on the revealed facts to the relevant state control bodies in the prescribed manner.

1666. Supervisors for leasing organizations and exchanges do not have the authority to impose the required sanctions. The ICR for Exchange Members (cl. 6 No. 2038 of 06.11.2009) stipulates that exchange trading rules approved by the exchanges shall provide for the application of proportionate measures in respect of exchange members who do not comply with AML/CFT legislation. These measures are reflected in the Rules of Exchange Trading: at UZEX (paras. 242-249), RUACE (Appendix No. 13, paras. 10-11).

Weighting and Conclusion

1667. The supervisory authorities for most FIs have the power to carry out inspections. Central Bank, commodity exchanges has, to a large extent, the authority request and check reports and other documents, request clarification of information, and impose sanctions for breaches of AML/CFT/CPF legislation. For the remaining supervisors the following deficiencies were identified: the supervisors for exchange members, professional securities market participants have no authority to conduct inspections; the supervisor of insurance companies does not have the power to request any information other than that requested during inspections; the set of sanctions from the Insurance Market Development Agency under the Finance Ministry is limited; Sanctions of the Ministry of Finance are not specified in case of identification of AML/CFT violations by securities market participants. Given the weight of these sectors, these shortcomings are assessed as minor.

1668. **Recommendation 27 is rated Largely Compliant.**

Recommendation 28 - Regulation and supervision of DNFBPS

1669. In the 2010 MER, Uzbekistan was rated under R.28 as "PC". There was no clear regulation of the powers of supervisors in the sectoral laws and regulations in terms of supervision and sanctions for casinos and other DNFBPS for non-compliance with AML/CFT measures, there were significant deficiencies in the licensing procedure and general monitoring of compliance with AML/CFT

measures. The legislation of Uzbekistan did not cover trusts and entities that create and service legal entities by appropriate measures.

Criterion 28.1

1670. There is a ban on casino activities in Uzbekistan. There is no legal regulation of the organisation of gambling and the illegal organisation of gambling is a criminal offence (article 278 of the CC); participation in gambling games not permitted by law is an administrative offence (article 191 of the CAO).

Criterion 28.2

1671. Pursuant to Art. 6 of the AML/CFT Law, ICRs for DNFBPs are developed and approved by the appropriate supervisory agencies in conjunction with the designated specialised state agency (FIU). In the absence of supervisory agencies ICRs are developed and approved only by the designated specialised state agency (FIU). Monitoring and control over compliance with the ICR is carried out by the bodies that approved these rules, namely:

- The Ministry of Justice together with the specially authorized state body for notary offices and lawyers' groups of the sector of notaries and lawyers (cl. 34 of the ICR of 19.10.2009 No. 2020, subparagraph19-1 cl.10 of the Regulation on the Ministry of Justice of the Republic of Uzbekistan approved by Presidential Decree No. PP-3666 of 13.04.2018);
- Finance Ministry and specially authorized state body for audit organizations (cl. 57 of the ICR of 15.12.2018 No. 3101, subparagraph 15, cl. 9 of the Regulation on the Ministry of Finance of the Republic of Uzbekistan, approved by Presidential Decree No. PP-2847 of 18.03.2017);
- Assay Chamber and specially authorized state authority for precious metals and stones dealers (cl. 27 of the ICR of 03.11.2009 No. 2034); responsibilities for monitoring AML/CFT legislation in the sector are also laid down in the regulation on the Assay Chamber (cl. 11 of Regulation of 16.08.2019 No. 677);
- State Asset Management Agency in conjunction with the designated state agency for realtors (cl. 30 of the ICR of 24.08.2011 No. 2257, cl. 10 of the Regulation on the State Assets Management Agency, approved by Resolution No. 404 of the Cabinet of Ministers of the Republic of Uzbekistan of 15 May 2019).
- Activities related to the provision of services related to the registration of companies (agent for the creation of legal entities) are not regulated by the AML/CFT/CPF legislation and no supervisory authority for such persons has been identified.

1672. In addition, in conjunction with the bodies that approved the ICRs the designated AML/CFT/CPF public authority, the DCEC is responsible for monitoring the compliance of legal entities and individuals with the AML/CFT/CPF legislation (Art. 9 of the AML/CFT Law, cl.7 of Regulation on the DCEC, cl.35 of the List of inspections carried out by notifying the authorised body by registering them in the Unified System of Electronic Registration of Inspections, approved by Presidential Decree No. UP-5490 of 27 July 2018). The powers of the DCEC also include monitoring the implementation of the ICR by organizations without interference in their economic activities (cl. 7 of Regulation on the DCEC).

Criterion 28.3

1673. The AML/CFT/CPF activities of DNFBPs are monitored by the state authorities that approve the sector's ICRs. Monitoring and supervision of compliance with internal control rules is carried out by the bodies that have approved these rules, as well as by the specially authorised state body. All categories of DNFBPs have appropriate supervisory bodies and are subject to monitoring and control in the context of AML/CFT/CPF compliance. The procedure for joint control and supervision is established by the Regulation on the procedure for monitoring and control of compliance with AML/CFT/CPF legislation by the entities conducting transactions with cash or other property (approved by Decree of the CM No.402 of 29.06.2021).

Criterion 28.4

1674. In accordance with the Regulation on the Procedure of Organization of Monitoring and Control of Compliance with AML/CFT/CPF legislation by reporting entities (approved by Decree of the CM No.402 of 29.06.2021) the assessment of compliance of DNFBPs may be carried out through monitoring or/and control.

1675. Monitoring refers to the totality of measures aimed at remote analysis of information and reports on the compliance with AML/CFT/CPF legislation by reporting entities. Control is the totality of measures aimed at examining the state of compliance with AML/CFT/CPF legislation requirements with a direct visit to the organization (cl. 2 of the Regulation).

a) Monitoring and control on compliance with AML/CFT/CPF legislation is carried out by competent authorities (cl. 3 of the Regulation).

   The DCEC controls and monitors all DNFBP sectors in accordance with the Regulation on the DCEC and DNFBP's ICRs (cl. 7 of Presidential Decree of 23.05.2018 No. UP-5446) and the AML/CFT Law (Art. 9). Resolution of the Cabinet of Ministers No.402 of 29.06.2021"On additional measures to implement the AML\CFT\CPF Law of the Republic of Uzbekistan " approved Regulations on the organization of monitoring and supervision of compliance by organizations engaged in transactions with cash or other property with legislative requirements for combating the legalization of income derived from criminal activity and the financing of terrorism and financing weapons of mass destruction proliferation, which establishes the procedure for monitoring and control and applies to all supervisory bodies.

   Also, by Presidential Decree No. UP-6252, dated 28.06.2021, an addition was made to Presidential Decree No. UP-5490, according to which the AML/CFT/CPF supervisory authorities are specified, along with the DCEC, as state bodies that approve ICR and the bodies charged with control.

   These regulations provide the DCEC and other supervisory authorities with the necessary powers to monitor and supervise DNFBPs' compliance with AML/CFT requirements.

b) The legislation contains a number of restrictions in order to prevent criminals (or their accomplices) from being professionally accredited or holding an interest in DNFBPs:

   - A notary and a lawyer cannot be a person with an unexpunged criminal record. In the case of a notary, there are also restrictions related to business reputation (cl. 2 of the Law "On Notaries" of 26.12.1996 No. 343-I, cl. 3 of the Law "On Advocacy" of 27.12.1996 No. 349-I).
   - In accordance with Art. 5 of the Law "On Audit Activity" of 26.05.2000 No. 78-II, the head of the audit organization should be an auditor for whom this audit organization is the main place of work, while according to Art. 25 of Law of 26.05.2000 No. 78-II, the reasons for termination of the auditor's certificate are revealed professional violations or a court verdict.
   - For the other sectors there are no required restrictions. For all sectors, there are no requirements for beneficial owners and controlling interest holders; the licensing requirements do not apply to affiliated persons. Supervisory authorities have no mechanisms to identify beneficial owners.

c) The CAO establishes responsibility for violations of AML/CFT law (Art. 1793 of the CAO). Responsibility for violations of industry norms is also provided:

   - Disciplinary responsibility is provided for notaries and lawyers (Article 19 of Law "On Notaries" of 26.12.1996 No. 343-I; Article 14 of the Law "On Advocacy" of 27.12.1996 No. 349-I). A lawyer's violation of the legislative requirements governing the legal profession, the professional conduct rules, lawyer's secrecy and the Lawyer's Oath entails the application of disciplinary measures against him (Article 4 of Law "On Advocacy" of 27.12.1996 No. 349-I). A lawyer may be subject to penalties up to and including decertification.
   - Responsibility for violation of license requirements and requirements of AML/CFT/PSMF legislation are established for audit organizations (article 46 of ZRU-677 of 25.02.2021, para. 9 sub-paragraph 15 of Decree No. PP-2847 of the President of the Republic of Uzbekistan of 18.03.2017).

- The Ministry of Finance has the right to take measures in case of violations of AML/CFT/CPF legislation (point 9, point 15 of Annex 7 of the Presidential Decision No. PP-2847 of 18.03.2017)
- A report for violation of AML/CFT/CPF legislation under Article 179-3 of the CAO is prepared by an official of the authorized agency and is filed to the administrative court for examination. According to CAO Art.15, executive officers, including directors and senior managers, of legal entities are held liable for administrative offences covered by CAO Art.179-3 on condition that they have breached a regulation whose enforcement is part of their official duties.

Criterion 28.5

1676. Established the requirement to carry out inspections based on the results of a "risk analysis" system involving the initiation of inspections based on the risk of committing violations of legislation (Clause 5 of Presidential Decree No. UP-5490 of 27.07.2017). The Regulation on the Procedure of Organization of Monitoring and Control of Compliance of Organizations Carrying out Transactions with Cash or Other Property with the Requirements of the AML/CFT/CPF Legislation (approved by Decree of the Cabinet of Ministers No.402 of 29.06.2021) provides for a mechanism of analysis and assessment of compliance of organizations with the requirements of the ICR and AML/CFT/CPF legislation based on the information obtained in the course of remote monitoring.

a) For some categories of DNFBPs, the frequency of inspections or the reason for inspections is determined, but these determinations are not conditioned by the risk-based approach (RBA). For notary offices, inspections are conducted every two and a half years (cl. 9 of Regulation approved by Order 367-UM of the Minister of Justice of 04.12.2018). For precious metals and stones dealers, auditing organizations and realtors, the conduct of inspections is associated with the possible risks of their violation of license requirements or in view of the complaints received (cl. 22 of Regulation approved by Resolution of the Cabinet of Ministers of 13.03.2019 No. 218; cl. 72 of Regulation approved by Resolution of the Cabinet of Ministers of 30.09.2017 No. 777, cl. 31 of Regulation approved by Resolution of the Cabinet of Ministers of 10.05.2011 No. 129). In the real estate sector, the State Asset Management Agency has adopted Order No 13-P of 25.01.2021 "On the Application of a Risk-Based Approach in the Implementation of Measures to Control the Compliance of Realtors' Activities with Legislation on Combating Money Laundering and Terrorist Financing". RBA is set in the Recommendation on applying the risk-based approach in the monitoring and control of compliance of insurance, leasing and auditing organizations, as well as precious metals and stones dealers, with AML/CFT/CPF legislation (approved by the Finance Ministry Working Group Protocol No. 2 of 06.02.2020). For audit organisations there is also remote access via the Audit PC (Article 12 of ZRU-677 of 25.02.2021) and the RBA is set in the Act on Auditing (Articles 47, 48 of ZRU-677 of 25.02.2021), which groups organisations into 3 categories according to their risk profile.

b) There is no information that supervisors should take into consideration (a) the type and number of supervised persons in the DNFBP category, (b) the extent of discretion allowed to them under the RBA.

Weighting and Conclusion

1677. The AML/CFT/PF monitoring and control obligations and rights apply to all supervisory authorities in view of the provisions of RCM-402 of 29.06.2021 and UP-6252 of 28.06.2021 and in accordance with the Regulations of the supervisory authorities and approved ICRs in all sectors. Supervision shall be in the form of monitoring and control and shall be carried out using the RBA. Restrictions on the management or ownership of DNFBPs by criminals exist only for a number of DNFBP sectors.

1678. However, there are no requirements for beneficial owners and persons owning controlling interests, and the licensing requirements do not apply to persons affiliated with criminals.

1679. **Recommendation 28 is rated Largely Compliant.**

Recommendation 29 - Financial intelligence units

1680. In the last MER, Uzbekistan was rated under the former R.26 as "Largely Compliant". The following deficiencies were identified: The authority of the head of the FIU raised questions regarding the

operational independence of the FIU. The FIU does not publish periodic reports on its performance. Inaccuracies in the wording of regulations regarding the authority of the FIU to request additional information could potentially lead to denial of the request.

Criterion 29.1

1681. The DCEC is defined as a specially authorized state body of the Republic of Uzbekistan on AML/CFT/CPF (cl. 1 of Presidential Decree of 23.05.2018 No. UP-5446), including collection and analysis of information on transactions in monetary funds or other assets to identify ML/TF/PF and related predicate offences (Art. 9 of Law of 26.08.2004 No. ZRU 660-II, cl. 11 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446). It is the national FIU and the only body with such functions.

1682. Besides that, the DCEC, if there are sufficient grounds or upon request, has the right to file materials on transactions in monetary funds or other assets related to ML/TF/PF to competent state authorities (Art. 9 of Law of 26.08.2004, No. ZRU 660-II).

1683. The DCEC is also the LEA, which carries out OIA, pre-investigative checks and inquiries into economic and corruption crimes, facts of ML/TF/PF.

Criterion 29.2

a) The DCEC receives and analyzes STRs, including attempted transactions, from reporting entities as per Recommendations 20 and 23 (Art. 13 and 15 of Law of 26.08.2004, No. ZRU 660-II). Reports are filed to the DCEC by using an automated set of software for data entry, processing and transmission with the use of cryptographic protection of information (cl. 10 of Regulation on the procedure of providing information related to AML/CFT approved by Resolution of the CM of 12.10.2009 No. 272). There are several types of incoming STRs: for suspicious transactions; for suspicious criteria fixed in the ICR and for criteria related to the List (29.2b).

b) The DCEC, within its competence, obtains other information stipulated by law, including on the transactions if one of the parties is (Art 14 of Law of 26.08.2004, No. ZRU 660-II):

- a legal or natural person involved in or suspected of involvement in terrorist activities or proliferation, including PF;
- a legal or natural person who directly or indirectly owns or controls an entity involved in or suspected of involvement in terrorist activities or proliferation, including PF;
- a legal entity that is owned or controlled by an individual or organization involved in or suspected of involvement in terrorist activities or proliferation, including the PF.

Criterion 29.3

a) The DCEC has a full set of powers enabling it to request, receive and use information received from state bodies, institutions conducting transactions in monetary funds or other assets, as well as officials and citizens to perform its functions (Art. 9 of Law of 26.08.2004 No. ZRU 660-II, cl. 12 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446). In particular, the DCEC has the right to file both primary and clarifying requests for additional information or clarifications from reporting entities (cl. 23 of Regulation approved by Resolution of the CM No. 272 of 12.10.2009).

b) The DCEC has access to a wide range of financial, administrative and law enforcement information, including access to databases of state agencies and telecommunications facilities and computer databases of organizations involved in transactions in monetary funds or other assets (Art. 9 of Law of 26.08.2004, No. ZRU 660-II, cl. 12 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446). Access is through government secure electronic communication channels E-HAT and LOTUS in the form of requests for necessary information (e.g., bank statements, customer information, tax information, etc.).

Criterion 29.4

a) The DCEC identifies predicate crimes, conducts operational analysis (Art. 9 of Law of 26.08.2004, No. ZRU 660-II), as well as systematic monitoring and financial analysis of STRs to identify ML/TF/PF indicators (cl. 5, cl. 11 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446).

b) Employees of the DCEC conduct strategic analysis by carrying out a comprehensive analysis of ML/TF/PF activities, and developing proposals for further improvement of legislation and law enforcement practice (Art. 9 of Law of 26.08.2004 No. ZRU 660-II, cl. 10 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446).

Criterion 29.5

1684. The DCEC, if there are sufficient grounds or upon request, is entitled to file materials on transactions in monetary funds or other assets related to ML/TF/PF (inluding the results of its analysis) to the competent state authorities (Art. 9 of Law of 26.08.2004 No. ZRU 660-II). The procedure for making inquiries and forms of feedback are established by agreements between the DCEC and competent authorities, as well as the Joint Instruction of the GPO, the MIA, the SSS and the SCC of 10.05.2021 "On the procedure for studying the financial aspects of criminal activity in the implementation of operational and investigative activities, pre-investigation, inquiry and preliminary investigation".

1685. Information is transferred via secure communication channels in accordance with interagency agreements between the DCEC and other competent authorities.

Criterion 29.6

a) The AML/CFT/CPF legislation of the Republic of Uzbekistan allows the DCEC and other competent bodies of the national AML/CFT/CPF system to restrict access to the related information (Art. 20 of Law of 26.08.2004 No. ZRU 660-II).Employees of the DCEC are obliged to ensure confidentiality and safety of information constituting commercial, banking and other secrets (Art. 19 of Law of 26.08.2004 No. ZRU 660-II, cl. 12 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446).

b) The DCEC ensures an appropriate level of access of its employees to classified information constituting commercial, banking and other secrets (Art. 19 of Law of 26.08.2004 No. ZRU 660-II, cl. 12 of Regulation on the DDCEC approved by Presidential Decree of 23.05.2018 No. 5446). In accordance with internal procedures, all employees of the DCEC are warned against responsibility for disclosure of information that became known to them in the course of their official duties. Liability for disclosure of confidential information and state secrets is envisaged by the criminal legislation of the Republic of Uzbekistan (Art. 162, 163, 191 of the CC).

c) Access to devices and information in the DCEC is provided by:

- Instruction of the Head of the DCEC "On ensuring information security in the use of computer equipment"of 24.12.2009 No. 8/203-09;
- Instruction of the Deputy General Prosecutor "On ensuring information security" of 11.08.2016 No. 26/ICT-24-16-7/75.

1686. All buildings and facilities of the DCEC are subject to protection by the National Guard of the Republic of Uzbekistan on the basis of Article 3 of the Law "On the National Guard of the Republic of Uzbekistan" and the agreement concluded between the DCEC and the National Guard.

Criterion 29.7

a) The DCEC is an independent specialized LEA (Presidential Decree of 23.05.2018 No. 5446, cl. 2 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446). The Head of the DCEC is appointed by the President of the Republic of Uzbekistan upon the proposal of the General Prosecutor (cl. 17 of Regulation o). The Head of the DCEC is accountable to the General Prosecutor (cl. 18 of Regulation), however, he has a fairly wide range of powers and autonomy to

perform his functions. The Head of the DCEC has full authority to make independent decisions on analysis, request and dissemination of information (cl. 2 of Presidential Decree of 23.05.2018 No. 5446). Interference in the activities of the DCEC and influence in any form on its employees in order to hinder the legitimate performance of the assigned tasks and functions is prohibited and entails liability established by law (cl. 23 of Regulation).

b) The DCEC has broad powers to interact with national and foreign competent authorities, international and other organizations for AML/CFT/CPF purposes, including the right to request and receive without charge and on the principles of reciprocity the necessary information (Art. 9 of Law of 26.08.2004, No. ZRU 660-II, cl. 2 of Presidential Decree of 23.05.2018 No. 5446, cl. 12 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446). The DCEC has concluded more than seven interagency agreements with law enforcement and other state bodies on cooperation, including on information sharing in the field of AML/CFT/CPF. In order to create a legal framework and expand interagency cooperation with foreign competent authorities, 22 agreements and memorandums on AML/CFT/CPF information exchange have been initiated and signed by the DCEC.

c) The DCEC, being a specially authorized state body in the field of AML/CFT/CPF in the Republic of Uzbekistan, performs the functions of the FIU (cl. 11 of Regulation on the DCEC approved by Presidential Decree of 23.05.2018 No. 5446).

d) The ВСУС is a legal entity and has a seal, as well as bank accounts opened in accordance with the law (cl. 6 of Presidential Decree of 23.05.2018 No. 5446). The head of the DCEC is personally responsible for its activities, approves the staff list, regulations on departments and divisions of the central office, as well as issues, within its authority, orders, instructions and directives on the organization of the department's activities, binding on all its employees (cl. 17-21 of Regulation).

Financial and logistical support of the DCEC is carried out at the expense of the State budget of the Republic of Uzbekistan and other sources not prohibited by law (cl. 17-21 of Regulation on the DCEC). The estimate of expenses of the DCEC is approved by the management of the FIU and the Ministry of Finance independently of the GPO. The DCEC created a special extra-budgetary fund to place free extra-budgetary funds in national and foreign currency, as well as funds on deposit accounts of the DCEC, on deposits in commercial banks of Uzbekistan (cl. 12 of Regulation on the DCEC). The availability of a special extra-budgetary fund of the DCEC contributes to obtaining additional resources for its activities and greater operational independence. 10 percent of the illegal spending of budgetary funds by state bodies and organizations, recipients of budgetary funds, theft, embezzlement, shortage revealed by the results of DCEC audits, inspections and recovered to the state budget and state trust funds of the Republic of Uzbekistan are credited to the special extra-budgetary fund of the DCEC.

Criterion 29.8

1687. The DCEC is a member of the Egmont Group since 01.07.2011.

Weighting and Conclusion

1688. **Recommendation 29 is rated Compliant.**

Recommendation 30 - Responsibilities of law enforcement and investigative authorities

1689. In the previous MER, the Republic of Uzbekistan was rated "LC" under former Recommendation 27 in terms of responsibilities of LEAs. The main deficiency was considered to be the impossibility to ascertain whether LEAs have relevant powers and functions due to the lack of possibility to analyze the legal framework regulating their activity (apart from the CPC).

Criterion 30.1

1690. In the Republic of Uzbekistan activities on detection, suppression and investigation of crimes are carried out in the form of OIA and pre-trial proceedings on criminal cases and materials. Pre-trial proceedings consist of two stages: pre-investigation check and investigation.

1691. OIA is the activity aimed at preventing, detecting, suppressing and solving crimes, as well as identifying and locating persons involved in their preparation and commission.

1692. Pre-investigative check includes measures to verify complaints, communications and other information concerning crimes and to take a decision on the outcome of the inquiry (institution of criminal proceedings or refusal to initiate them, or referral of the complaint or communication to the appropriate investigative jurisdiction), as well as measures to secure and preserve traces of crimes, objects and documents which may be of significance in a criminal case.

1693. Investigation of a criminal case consists in the direct collection, preservation and assessment of evidence in a criminal case and, depending on the type of crime committed, is carried out either in the form of an inquest or in the form of a preliminary investigation.

1694. Depending on the complexity of the crime, its detection, solving and investigation may take several forms (e.g., OIA, pre-investigative inquiry and preliminary investigation) or one form (e.g., preliminary investigation).

1695. Bodies involved in criminal intelligence and detective operations are defined in the Law of the Republic of Uzbekistan of 25.12.2012 No. ZRU-344 "On Criminal Intelligence and Detective Operations" (hereinafter – Law of 25.12.2012 No. ZRU-344). In accordance with Article 10 of this law, criminal intelligence and detective operations are carried out by the MIA, the SSS, the State Security Service of the President of the Republic of Uzbekistan, military intelligence of the Defence Minisrty, the SCC, the Department for Combating Economic Crimes under the GPO of the RU and the Compulsory Enforcement Bureau under the GPO of the RU.

1696. Based on the provisions of Articles 10 and 15 of Law of 25.12.2012 No. ZRU-344, detection and solution of ML and TF crimes may be carried out by any body involved in criminal intelligence and detective operations.

1697. Bodies responsible for conducting pre-investigative checks and investigating criminal cases are determined by the CPC.

1698. In accordance with Articles 38 and 381-2 of the CPC, the investigation of criminal cases of certain types of predicate offences (listed in Article 381-2 of the CPC) in the form of inquiries is carried out by the inquirers of the internal affairs bodies, the BCE and its local units, the DCEC and its local units, the SCC and its local units, the National Guard and its local units.

1699. Criminal cases of other predicate offenses (except TF) are prosecuted in the form of preliminary investigations by investigators of the prosecutor's office, internal affairs bodies, and the SSS (Article 345 of the CPC).

1700. Preliminary investigation in TF criminal cases is carried out by investigators of the SSS.

1701. Preliminary investigation in ML criminal cases is carried out by investigators of internal affairs bodies (MIA).

1702. Pursuant to Article 345 of the CPC, if the investigation reveals a new crime that is under the jurisdiction of another preliminary investigation body, the investigation may, with the prosecutor's consent, be completed in its entirety by the preliminary investigation body that has jurisdiction over the case. When criminal cases under investigation by different preliminary investigation bodies are merged into one proceeding, the prosecutor shall assign the investigation to the body which has jurisdiction over the criminal case involving the more serious offence and, if the nature and degree of public danger of the offences are equal, to the body which investigates the criminal case for the longest period of time.

1703. Besides that, the General Prosecutor of the Republic of Uzbekistan or his deputies, in order to ensure comprehensiveness, completeness and objectivity of the investigation, shall have the right to transfer a criminal case from one preliminary investigation body to another, regardless of the rules of investigative jurisdiction in cases provided for by law.

1704. Thus, under certain circumstances ML cases may be investigated by bodies other than internal affairs bodies.

1705. Pre-investigative checks are carried out by bodies authorized to investigate relevant crimes, as well as by the STC Main Directorate for the Prevention of Offenses in the Field of Retail Trade and the Provision of Services, border guard authorities and other state bodies listed in Article 39-1 of the CPC.

Criterion 30.2

1706. In accordance with Articles 321 and 322 of the CPC, the reasons for initiation of criminal proceedings, i.e. the commencement of an inquiry or preliminary investigation, are statements by persons, reports by enterprises, institutions, organizations, public associations and officials, mass media reports, discovery of information and traces indicating a crime, directly by the inquirer, investigator, prosecutor, as well as the preliminary investigation body, a statement to confess. In this connection, inquirer, investigator, prosecutor, as well as the official of the preliminary investigation body are obliged, within the limits of their jurisdiction, to institute criminal proceedings for the crime in all cases where there are reasons and sufficient grounds for doing so.

1707. Thus, investigations into predicate offenses as well as ML/TF may be conducted on the basis of any sufficient information about its commission, including the results of a parallel financial investigation, if any.

1708. There are no provisions in national law that prevent parallel financial investigations from being conducted either concurrently with or separately from the investigation of predicate offenses and ML. The prosecuting authority may entrust certain elements of parallel financial investigations (audit, expertise, etc.) to agencies involved in criminal intelligence and detective operations, or to other competent authorities and organizations.

1709. The procedure for studying financial aspects of criminal activity (parallel financial investigations) in the course of criminal intelligence and detective operations, pre-investigative checks, inquest and preliminary investigation is defined by the Joint Directive of GPO, MIA, SSS and SCC of 10.05.2021 "On investigating the financial aspects of criminal activity in the course of criminal intelligence and detective operations, pre-investigative checks, inquest and preliminary investigation". According to clause 4 of the Guidelines, parallel financial investigations are mandatory for ML offences (including if the predicate offence was committed outside the RU), TF offences and offences resulting in particularly large damage or income on a particularly large scale.[134] In other cases, parallel financial investigations are conducted at the discretion of the competent authorities, with priority being given to predicate offences which are classified by the NRA as having a "very high" and "high" ML threat level. Before adopting this joint directive, the LEAs were guided by general provisions in the CPC on the need to establish the extent of the damage caused, ensure reparation, and ascertain the property status of the accused (suspect) during the investigation. A separate regulation only existed in the SSS (of limited distribution).

1710. The joint directive also determines the set of measures by which parallel financial investigations are conducted, the amount of data to be established, the procedure for cooperation of the authorized bodies, and other issues.

Criterion 30.3

1711. Under the Joint Directive on investigating the financial aspects of criminal activity, prosecutors, MIA, SSS, and SCC are authorized to identify and trace proceeds of crime, TF funds, items and other crime and other assets, including the property of equivalent value, which may be subject to conversion to state revenue and confiscation at any stage of the OIA, pre-investigative check, inquest, and preliminary investigation.

[134] According to Section 8 of the CC, large damage (criminal income) is an amount from 300 to 500 RSV, which at the USD exchange rate as of 02/07.2021 is equivalent to an amount from 6,900 to 11,500 USD, while particularly large damage (income) is an amount over 500 RSV, i.e. exceeding 11,500 USD.

1712. Before the adoption of the above-mentioned inter-institutional act, as at present, the obligation for the preliminary investigation authorities to establish the extent of the damage caused was envisaged in CPC as the circumstances necessary for a conviction (Article 82 of the CPC).

1713. Identification and tracing of property subject to confiscation prior to initiation of a criminal case are carried out within the framework of OIA by all its authorities within their competence.

1714. When criminal proceedings are initiated, the identification of property liable to confiscation is carried out by the preliminary investigation authority through investigative operations such as seizure (Article 157 of the CPC), searches (Articles 158, 161 and 162 of the CPC), and examinations of the scene of events, locations, premises, objects and documents (Articles 135-141 of the CPC).

1715. The obligation to identify and seize property to enforce property penalties (including confiscation) is imposed on all bodies listed in Criterion 30.1, which conduct preliminary investigation during pre-trial proceedings (Article 290 of the CPC). The seizure of property cannot be applied before the initiation of criminal proceedings.

1716. Pursuant to Article 9 of the AML/CFT/CPF Law, the DCEC is authorized to issue orders to suspend transactions in monetary funds or other assets for a period not exceeding thirty business days to implement measures aimed at combating money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

1717. In accordance with the Regulation on the DCEC approved by Presidential Decree No. 5446 of 23.05.2018 "On measures to radically improve the efficiency of the use of budgetary funds and improve mechanisms to combat economic crimes", the DCEC, if there are sufficient grounds, takes measures to suspend transactions and (or) freeze cash and other assets of persons suspected of committing economic crimes, ML, TF, PF. The procedure for sending orders to suspend transactions in monetary funds or other assets by the DCEC is determined by the order of the Head of the Department of 01.02.2021 No. 3.

1718. Thus, for these types of predicate offenses and under ML/TF/PF the DCEC is empowered to suspend transactions and freeze property, including at the stage of conducting OIM.

Criterion 30.4

1719. The legislation of the Republic of Uzbekistan provides state bodies, which are not LEAs per se, but are responsible for conducting financial investigations of predicate offences, with the powers of LEAs within their competence.

1720. For example, STC is a state administration body and is not a LEA. However, the STC Main Directorate for the Prevention of Offenses in the Field of Retail Trade and the Provision of Services is a body involved in pre-investigative checks of offenses in the financial-economic and tax spheres revealed on the territories of markets, shopping complexes and adjacent to them places of temporary storage of vehicles. When conducting pre-investigative checks, the head of the said body has the powers stipulated in Articles 39-2 and 329 of the CPC (to detain a person, search him or her personally, seize and request documents, inspect the scene of the crime, order an audit, order to conduct OIA, initiate a criminal case), along with other bodies involved in pre-investigative checks, including LEAs.

Criterion 30.5

1721. According to Article 7 of the Law "On Combating Corruption"[135] the bodies involved in combating corruption are the GPO, the SSS, the MIA, the Ministry of Justice, the DCEC.

1722. These bodies, with the exception of the Ministry of Justice, are preliminary investigation bodies and conduct criminal proceedings on predicate offenses, including those related to corruption. As noted in Criteria 30.1 and 30.3 ML is referred to the jurisdiction of internal affairs bodies. However, under certain circumstances, all of the noted bodies (except the Ministry of Justice and the DCEC) may investigate ML. Identification, tracing, initiation of freezing and seizure of property, which is the

[135] Law of the Republic of Uzbekistan of 03.01.2017 No. ZRU-419 "On Combating Corruption".

proceeds of crime or is (may be) subject to confiscation is the responsibility of the bodies empowered to investigate ML.

1723. The Ministry of Justice does not investigate crimes and is not a law enforcement agency.

1724. The Law "On Combating Corruption" also authorizes the DCEC to conduct criminal intelligence and detective operations, pre-investigative checks and inquiries into ML, economic and other corruption-related crimes. However, there are no relevant provisions on the performance of inquiries on ML crimes in the CPC, nor is there any provision for investigating ML crimes (Article 243 of the CC) in the form of an inquest.

Weighting and Conclusion

1725. **Recommendation 30 is rated Compliant.**

Recommendation 31 - Powers of law enforcement and investigative authorities

1726. In the 2010 MER, Uzbekistan was rated under former R.28 in terms of responsibilities of law enforcement and investigative authorities as "Compliant".

Criterion 31.1

1727. As previously noted, preliminary investigations in criminal cases of TF are conducted by investigators of the SSB, in criminal cases of ML crimes – by investigators of MIA bodies. However, the investigation of such cases in certain cases can also be carried out by other preliminary investigation bodies. The detection and investigation of predicate crimes is carried out by the relevant authorized law enforcement and investigative agencies (see Criterion 30.1).

1728. When conducting OIA, inquest and preliminary investigations in criminal cases of predicate offenses, ML and TF, LEAs use a significant amount of authority.

a) In accordance with Article 201 of the CPC, the heads and other officials of enterprises, institutions, and organizations shall, at the request of an inquirer, investigator, prosecutor or court, provide documents in their possession or specially compiled on the basis of the information they have. Forcible seizure of documents is carried out in the course of a seizure or search (Articles 157 and 158 of the CPC). Searches of premises must be authorised by a prosecutor but, in urgent cases, may be carried out without such authorisation, but with notification to the prosecutor within 24 hours. No authorisation is required for the seizure of documents or for the compulsory production of documents. Thus, records held by FIs, DNFBPs and other individuals and legal entities may be obtained both on the basis of a request by an inquirer, investigator, prosecutor or court for the production of documents and also during a seizure or search. When conducting OIA to detect and suppress crimes, authorized bodies may obtain information held by financial institutions, DNFBPs and other individuals and legal entities by carrying out investigatory actions such as "making inquiries" and "inspection of residential and other premises, buildings, structures, areas and vehicles". Such activities may be carried out both publicly and privately (Articles 9 and 14 of Law of 25.12.2012 No. ZRU-344).

b) During the preliminary investigation in criminal cases, all residential, business, industrial and other premises may be searched, and persons may be personally searched (Art. 158, 161 and 162 of the CPC). Legislation also provides for inspecting the scene of the crime, premises, items and documents to find traces of crime and material evidence and to establish the context of the incident and other circumstances relevant to the case (Art. 135-141 of the CPC). In the course of OIA, the "inspection of residential and other premises, buildings, structures, areas and vehicles" OIM is used (Art. 14 of Law of 25.12.2012 No. ZRU-344).

c) Evidence is taken by questioning witnesses, suspects and defendants (Chapters 10-12 of the CPC). Interrogations can be initial and supplementary. Witnesses are obliged to state what they know about the circumstances of the crime (Article 118 of the CPC). In the process of OIA, a "questioning" investigatory action is carried out (Article 14 of Law of 25.12.2012 No. ZRU-344).

d) The law provides for a procedural order of the evidence collecting and recording (Articles 203-207 of the CPC). The discovery, collection and seizure of physical evidence are provided for during examinations, searches and seizures (see above). The interrogated person may use documents during the interrogation which may be admitted as evidence after the interrogation (Article 103 of the CPC). Material evidence may be seized if found during the testimony (Articles 132-133 of the CPC). Physical evidence may be provided with materials of criminal intelligence and detective operations (OIA) (Article 19 of Law of 25.12.2012 No. ZRU-344).

Criterion 31.2

1729. The range of investigative techniques available to competent authorities is quite broad. They are defined by criminal procedural legislation (procedural actions), legislation on OIA (operational-investigative means) and regulations governing the powers and scope of activities of a particular body (specific powers).

1730. All covert activities are carried out within the framework of criminal intelligence and detective operations (Law of 25.12.2012 No. ZRU-344). They may be carried out by bodies authorized to conduct OIA, both on their own initiative and on behalf of the inquirer, investigator or prosecutor (Art. 36, 38-1 of the CPC). Thus, bodies of inquiry and preliminary investigation have the opportunity to use the mechanisms of covert activities by entrusting their implementation to bodies authorized to conduct OIA.

1731. Materials of OIA may be the basis for a criminal case or submitted to the inquiry and investigation bodies and prosecutor for use in criminal cases as evidence (Article 19 of Law of 25.12.2012 No. ZRU-344).

a) The list of OIM (covert operations) is defined in Article 14 of Law of 25.12.2012 No. ZRU-344. They include: (i) questioning, (ii) making inquiries, (iii) collecting samples for comparative analysis, (iv) test purchase, (v) controlled acquisition, (vi) examination of objects and documents, (vii) operational observation, (viii) identification, (ix) inspection of residential and other premises, buildings, constructions, areas and vehicles, (x) monitoring of postal, courier, telegraphic and other communications, (xi) wiretapping of telephones and other communication devices, (xi) retrieving information from technical communication channels, (xii) operational infiltration, (xiii) controlled delivery, (xiv) undercover operation, (xv) operational experiment.

b) Communications intelligence is provided for in Articles 169-10 of the CPC (interception of conversations conducted by telephone and other intercommunication devices) and Articles 166-167 of the CPC (seizure of postal and telegraphic communications). The communications intelligence actions include (i) monitoring of postal, courier, telegraphic and other communications, (ii) interception of conversations conducted by telephones and other communication devices, and (iii) retrieving of information from technical communication channels (Article 14 of Law of 25.12.2012 No. ZRU-344**).**

c) For access to computer systems, the "retrieving of information from technical communication channels" investigatory action is envisaged and used.

d) Controlled deliveries, depending on the circumstances and their purpose, are carried out as part of such investigatory actions as "controlled delivery" and "controlled acquisition". For more complex, comprehensive covert operations involving controlled deliveries, the "operational experiment" investigatory action is used.

Criterion 31.3

1732. The legislation regulates legal mechanisms for identifying accounts held or controlled by natural or legal persons, as well as ensuring that the competent authorities have a procedure for identifying assets without prior notice to the owner.

a) Information on operations, accounts and deposits of their customers (correspondents) are referred to bank secrecy. Such information is provided to the preliminary investigation authorities; bodies involved in OIA, with the prosecutor's authorization, and to the court on the basis of his written request. It is

possible to receive information constituting bank secrecy from the Central Bank database in an automated mode as well as by the same bodies and courts in the form of an electronic document via an information system and secure communication channels. LEAs also can receive information about accounts and deposits held with the FIU upon request on the basis of signed agreements on cooperation. In accordance with Article 5 of Law of the Republic of Uzbekistan of 30.08.2003 No. 530-II "On Bank Secrecy" such exchange of information constituting bank secrecy between prosecution, preliminary investigation, inquiry and investigative bodies, as well as the competent authorities of foreign states in accordance with the legislation and international treaties of the Republic of Uzbekistan shall not be considered a disclosure of bank secrecy.

b) Obtaining information on the existence of assets is carried out on a procedural basis by making inquiries, obtaining information from electronic databases and conducting searches (Articles 157, 158 and 203 of the CPC). When carrying out OIA, information on availability of assets can be obtained from electronic databases or by conducting the "making inquiries" investigatory action (Article 14 of Law of 25.12.2012 No. ZRU-344). Besides that, LEAs for obtaining information on assets also exercise specific powers granted to them by normative legal acts regulating the powers and scope of activities of a particular body, for example, the powers of the DCEC (FIU) to request and obtain necessary information, including from automated reference systems and databases, free of charge. The legislation of the Republic of Uzbekistan does not require the owner of assets to be notified in advance of the identification procedure by competent authorities.

Criterion 31.4

1733. Article 9 of the AML/CFT/CPF Law provides for the DCEC (FIU) to proactively or upon request file materials on transactions in monetary funds or other assets related to legalization of proceeds of crime, TF and PF to relevant authorities involved in combating ML, TF and PF. The FIU jointly with law enforcement and other state authorities shall determine the procedure for interaction on exchange and transfer of information and data related to the legalization of proceeds of crime, TF and PF.

1734. Similarly, bodies of the criminal investigation (MIA, GPO, SSS) and OIA units, when conducting preliminary investigation and carrying out OIM on ML cases and materials have the right, in accordance with the legislation regulating their activities, to request from the FIU the information necessary for the investigation.

1735. More detailed issues of interagency cooperation and execution of mutual obligations of the DCEC, MIA, STC and SCC are defined in joint Regulation on the cooperation procedure (Resolution of MIA and the DCEC of 06.02.2019 No. "On Approval of Regulation on the Procedure of Cooperation between the Internal Affairs Bodies and the DCEC" (MIA No. 8 of SC of 06.02.2019, DCEC No. 4 of 06.02.2019), Resolution of the DCEC and STC "On Approval of Regulation on the Procedure of Cooperation between the Bodies of the DCEC with the State Tax Service" (DCEC No. 5/1 of 18.02.2019, STC No. 2019-31 of 18.02.2019), Resolution of SCC and the DCEC "On Approval of Regulation on the Procedure of Cooperation between the State Customs Service Bodies and the DCEC" (SCC No. 01-02/4-42dsp of 24.06.2019, DCEC No. 19dsp of 24.07.2019)).

Weighting and Conclusion

1736. Recommendation 31 is rated Compliant.

Recommendation 32 – Cash couriers

1737. In the last MER, the Republic of Uzbekistan was rated under the former Special Recommendation 9 as "Partially Compliant". As the main deficiencies that affected the rating, assessors noted that the customs system in general is not applied for AML/CFT purposes; customs authorities lack the authority to request information from persons regarding the origin of funds/ bearer negotiable instruments and their intended use, and the authority to seize or detain funds in case of suspicion of ML or TF.

Criterion 32.1

1738. The Republic of Uzbekistan applies a declaration system for cross-border movement of currency and bearer negotiable instruments (BNI), the procedure for which is established by Chapter 37 of the Customs Code.

1739. The declaration procedure is as follows:

- registration of a passenger customs declaration when importing (exporting) the national currency of the Republic of Uzbekistan and currency valuables, goods of individuals for non-commercial purposes;
- drawing up a cargo customs declaration when importing (exporting) goods transported across the customs border in a separate luggage, which is imported or exported before or after the departure of an individual (cargo shipment).

1740. In accordance with Art. 13 of the Customs Code, the goods are any movable property conveyed across the customs border, including the national currency of the Republic of Uzbekistan, currency values and other securities, while securities include: bonds, bills, checks, deposit and savings certificates, bill of lading, shares and other documents (Art. 96 of the Civil Code).

1741. Cash currency of the Republic of Uzbekistan and foreign currency are included in the list of items and substances which are prohibited and restricted for remission by domestic and international postal and courier services (Rules for the Provision of Postal Services Reg. No. 2219 of April 18, 2011).

1742. Resolution of the President of the Republic of Uzbekistan dated 19/07/2018 "On measures to ensure control of goods import to the territory of the Republic of Uzbekistan to natural persons in international postal and courier parcels" approved the list of information to be submitted by postal operators and providers to customs authorities when pre-declaring such goods electronically. Order of the SCC No.351 of 19/11/2018 put into effect AIS "E-Commerce", through which the electronic declaration of international consignments is carried out.

1743. Resolution of the CM No. 814 of 11/10/2017 approved the Regulation on the application of double corridor system in the customs border crossing points of the Republic of Uzbekistan, which is applied in the international airports of the Republic of Uzbekistan – from 01.01.2018, in road and rail checkpoints across the customs border – from 01.01.2021. The said system gives a natural person the right to choose the order of crossing the customs border:

- through the "green corridor", when the declaration of goods (except for goods whose import and export is prohibited or restricted by law) is made orally – the passage through the "green corridor" is considered as a statement to the customs authority about the absence of goods subject to declaration;
- through the "red corridor", when the declaration of goods is carried out by filling out passenger customs information (Art. 162 of the Customs Code).

Criterion 32.2

1744. The Republic of Uzbekistan establishes a written form of declaration for all individuals moving cash currency in excess of the threshold value.

1745. Rules for import and export of foreign cash currency of the Republic of Uzbekistan and foreign cash currency by individuals across the customs border of the Republic of Uzbekistan approved by the Resolution of the CM of 30.01. 2018 No. 66 (as amended and supplemented by Resolution of 10/08/2020).

1746. According to the mentioned rules, cash currency (of the Republic of Uzbekistan and (or) foreign currency) imported and exported by individuals in excess of the amount equivalent to 70 million soums is subject to customs declaration, which is carried out in writing by filling out a passenger customs declaration for customs control purposes. Thus, the threshold amount for cash currency is about 6.600 USD (at the rate of 26/05/2021).

1747. The procedure for declaring foreign and national currency in cash and currency valuables is determined by the Instruction on the procedure for completing and executing the passenger customs declaration (SCC reg. MJ-2606 of 05/08/2014).

1748. By the Law No. 573 of 22/10/2019 "On currency regulation" currency valuables include securities and payment documents whose face value is expressed in foreign currency, non-denominated securities issued by non-residents. Thus, the threshold declaration system applies to BNIs.

Criterion 32.3

1749. The threshold declaration system is applied in the country.

Criterion 32.4

1750. The customs declaration is subject to customs control (Art. 178, 187 of the Customs Code). The forms of customs control include inspection of documents and information, verbal questioning, as well as obtaining information, which means that a customs official obtains the necessary information from authorized and other persons who have information about circumstances relevant to customs control (Art. 192 of the Civil Code).

1751. Under the Resolution of the SCC reg. MJ-2606-6 dated 05/08/2014 "On approval of the Instruction on the procedure for completing and executing the passenger customs declaration" (amended on 10/05/2021), the customs authorities are empowered to request information on the origin of currency in transit.

Criterion 32.5

1752. Failure to declare or inaccurate declaration shall lead to administrative or criminal liability.

1753. Under Article 227-22 of the CoAO, a natural person can be fined from 5 to 10 RSV (from USD 115 to 230)[136], and an official can be fined from 7 to 15 RSV. As an additional penalty, the sanction provides for confiscation of goods.

1754. Non-declaration or declaration of a wrong name committed on a large scale (for an amount from USD 6,900 to 11,500), following the application of an administrative penalty for the same violation, shall entail criminal liability. The mentioned act is punishable under Article 182 part 1 of the CC by a fine (up to $6,900), or community service (for up to 480 hours), or correctional labor for up to 2 years), or restriction of freedom for 2 to 5 years), or imprisonment for up to 5 years.

1755. Violation of customs laws in an especially large amount (ie, over USD 11,500) or other aggravating circumstances under Part 2 of Art. 182 of the CC is punishable by fine (ranging from USD 6,900 to 13,800), or correctional labor for up to 3 years, or imprisonment from 5 to 8 years.

1756. The sanctions provided for in the legislation are generally proportionate and dissuasive.

Criterion 32.6

1757. The customs authorities submit to the DCEC information on illegal import and export of cash in national and foreign currency (Art. 242 of the Customs Code).

1758. SCC provides monthly summary information to STC on violations of the established procedure for currency transactions (export-import operations, transfer of funds, etc.), on the basis of which the tax authorities conduct inspections and desk audit. When cases related to ML and TF are identified, the tax authorities notify the DCEC within 3 days (STC, SCC and CB Resolution of 12.06.2013 No. 2467).

1759. Interaction on exchange of information obtained as a result of declaration between the DCEC and the SCC is regulated by an interagency agreement on cooperation, as well as a joint Regulation on the interaction procedure (SCC No. 01-1/4-0525 DSP of 07.06.2021).

1760. Based on the mentioned interdepartmental acts, the DCEC is provided with online access to the SCC databases (information on passengers' declarations and cargos declarations).

[136] Hereinafter all amounts are based on the exchange rate current as of July 2, 2021.

Criterion 32.7

1761. The principle of carrying out tasks by customs authorities in cooperation with state bodies and other organisations is stipulated by Article 5 of the Law of 18.10.2018 No. LRU-502 "On the State Customs Service".

1762. In accordance with the Regulation on the SCC, approved by Resolution of the Cabinet of Ministers of 30.07./1997 No. 374 (as amended by Resolution of the CM of 29/06/2021 No. 402), the SCC interacts with the authorized state body (FIU) to counteract ML/TF/PF

1763. The procedure of interaction between customs authorities and the DCEC is regulated by the Regulation approved by a joint decision of the SCC and the DCEC (No. 01-1/4-0525 DSP of 07.06.2021).

1764. The mechanism of cooperation between the relevant government agencies in monitoring currency transactions is stipulated by STC, SCC and CB Resolution No. 2467 of 12.06.2013.

1765. Interaction with the CB is carried out through the SCC's Automated Information System "Passport Customs Declaration" (AIS PCD), which contains information on such declarations and the volumes of currency imported more than the statutory standards.

1766. Interaction between the SCC and the Border Guard Service of the SSS (Migration Service) is based on the Memorandum on Mutual Information Exchange (concluded on 17.12.2020). The exchange of information between the agencies takes place online (information systems AIS PCD, AIS Auto).

1767. Moreover, according to the information provided by the assessed country, cooperation with the SSS and MIA is carried out within the framework of joint Action Plans aimed at suppressing illegal import and export of goods, material values, smuggling of weapons, narcotic drugs and psychotropic substances.

1768. Mutual exchange of information with the STC, including information on goods received by natural persons in international postal items, is carried out by the SCC based on an inter-agency cooperation agreement concluded on 20/01/2020.

1769. The Memorandum of Cooperation on Information Exchange between the MIA and the SCC of 19/03/2020 provides for the exchange of data, including information from the AIS "Violations of Customs Laws" and others.

Criterion 32.8

a) According to Art. 4 of Law of 18.10.2018 No. LRU-502, the task of customs authorities is to counteract customs offenses and smuggling. As such, the powers of the customs service may only be used for these narrowly specific purposes. Customs authorities have the power to detain and seize goods that are the direct subjects of customs offenses (Art. 7 of Law of 18.10.2018 No. LRU-502).

Decree of the CM of 29/06/2021 No. 402 has amended the Regulation on the SCC (approved by Decree of the CM of 30/07/1997 No. 374), according to which the SCC is empowered to detain and seize cash or other property transferred across the customs border if there is suspicion and information about its involvement in ML/TF/PF.

b) In identifying offenses related to the illegal import and export of national cash currency of the Republic of Uzbekistan and foreign currency, the customs authorities seize illegally imported and exported currency, conduct investigative checks and initiate administrative or criminal proceedings (Art. 242 of the Customs Code).

Criterion 32.9

1770. The Customs Code defines a general period of keeping customs declarations, which is 3 years after the year in which goods lose their status as being under customs control. The customs legislation of the Republic of Uzbekistan does not provide for separate requirements for keeping information in cases of (b) inaccurate declaration and (c) suspected ML/TF.

1771. The customs declarations contain information both on the amount declared and on the identity of the bearer. According to the information provided by the country, passenger customs declarations are

kept in paper and electronic form (Automated Information System "Passenger Customs Information "AIS PTD""), and the period of keeping passenger customes imfprmation in electronic form is not limited.

1772. If the original of the false declaration is attached to the materials of a criminal or administrative case, the customs authorities keep a copy of the passenger customes information. In this regard, customs authorities have the opportunity to provide the necessary information as part of international cooperation.

Criterion 32.10

1773. Customs authorities are obliged not to disclose information constituting state secrets or other secrets protected by law that have become known to them in the performance of their official duties (Art. 8 of Law of 18.10.2018 No. LRU-502). The information collected through declaration systems shall be used for customs control purposes.

1774. Such information is filed by customs authorities to the DCEC – when detecting facts of illegal import or export of cash national and foreign currency and to STC – when detecting signs of violations of currency legislation (Art. 242, 245 TC).

Criterion 32.11

1775. Persons committing physical cross-border transportation of currency and BNI are subject to administrative and criminal liability, provided that their actions constitute an offence under Art. 227-22 of the CAO, or a crime under Art. 182 of the CC.

1776. In cases where the cross-border movement of currency and BNI is related to ML/TF or predicate offences, the individual may be held criminally liable including cumulative offenses.

1777. Sanctions for predicate offences depend on their gravity. The commission of grave crimes carries a penalty of imprisonment from 5 to 10 years, for especially grave crimes – from 10 to 20 years (Art. 15 of the CC).

1778. The most severe liability is established for terrorism, from 15 to 25 years of imprisonment or life imprisonment (Part 3 of Art. 155 of the CC).

1779. Thus, on the whole, the sanctions in the CC are proportionate and dissuasive.

1780. Administrative and criminal procedure laws (Art. 23 of the CAO, Art. 211, 284 of the CPC) provide for confiscation of the object of the offense (crime). Accordingly, currency and BNIs whose cross-border movement involves failure to declare or false declaration are subject to confiscation, which correlates with the measures in the context of Recommendation 4.

Weighting and Conclusion

1781. **Recommendation 32 is rated Compliant.**

Recommendation 33 - Statistics

1782. In the 2010 MER, Uzbekistan was rated partially compliant with former R.32, as no statistics were available regarding the amount of property frozen under the UN Security Council Resolutions, no separate statistics were maintained regarding the offences covered by the CC Art.155 (financing of terrorism), and no statistics were available regarding inspections conducted and sanctions applied by the supervisory authorities (except for the CB).

Criterion 33.1

a) The DCEC maintains databases and keeps statistics on STRs received, processed and disseminated (Article 9 of the AML/CFT Law) and unified centralized statistical records and reporting on its activities (par.8, 11 of the Regulation on the DCEC).

b) In accordance with the Decree of the President of the Republic of Uzbekistan from 31.10.2018 UP-5566 "On measures to radically improve the system of criminal-legal statistics and increase the systematic analysis of crimes" from 01.12.2018 the unified record of crimes, persons who have

committed them, movement of criminal cases is attributed to the competence of the GPO. This Decree provides for the development and implementation of the Unified Information System "Electronic Criminal Statistics" (hereinafter referred to as UIS) from 01.03.2019.

Presidential Decree No. UP-6196 of 26.03.2021 "On measures to raise to a qualitatively new level the activities of internal affairs bodies in the sphere of ensuring public security and combating crime" attributed the maintenance of the UIS to the competence of the MIA.
In accordance with the above-mentioned regulations, statistics are maintained:

- By the body which investigated the criminal case – on criminal prosecution at the entire stage of pre-trial proceedings in ML/TF cases (detection, disclosure, investigation and prosectution ML/TF), including data on the means of committing a crime, procedural decisions taken on the case, including decisions on the seizure of property;
- By the court hearing the case – the outcome of the trial (conviction, acquittal, discontinuation), the final procedural decision taken on the case, including the qualification of the offence, the type and amount of the penalty (if convicted), and the resolution of the seizure of the property;
- By the State bodies responsible for enforcing court decisions – on the enforcement of court decisions relating to property claims, compensation for damages to victims, and confiscation of property to the State.

The information provided by the country shows that the electronic statistical card on a criminal case reflects the amount of damage caused by the crime, but does not include the amount of proceeds of crime.
For TF offences, the statistics report the source of funding, the means of fundraising and TF, and the type of terrorist activity for which funds were raised or provided.
For ML crimes, the statistics do not reflect the ML type (self-laundering, ML by third parties); the kind of predicate offence; the amount of the laundered proceeds. Information on these types of data may be received by analysing the description (plot) of the committed crime.
Thus, the statistics on ML investigations are not comprehensive.

c) The DCEC keeps the records of frozen assets as part of its obligation to maintain the consolidated statistics and reporting records related to its activities (Presidential Decree No.5446 of 23.05.2018, sub-para 8 para11). The DCEC receives such information by means of STRs sent from institutions according to para 26 of the Regulation in the Order of the Prosecutor General No. 22-B of 11.10.2016), for which a separate opcode is allocated.

The procedure for recording seized property subject to forfeiture to the state, including instrumentalities, items, physical evidence in criminal cases and cases of administrative offences, property seized during the preliminary investigation to secure property penalties under sentences, is carried out under the Resolution of the Cabinet of Ministers No. 200 of 15.07.2009.

The authority that seized it shall keep maintaining statistics of the seized property and its movement during the pre-justice procedure.

Statistics on property seized during the preliminary investigation are kept by type of property (real estate, vehicles, bank accounts, etc.). However, seized property is not distinguished by the type in the context of Recommendation 4 (laundered property, instrumentalities and means of crime, property of the corresponding value).

Maintaining statistics on the execution of decisions of the court, other authorised bodies on confiscation of property to the benefit of the state is carried out by the BPI which keeps data on the transfer of property for realisation to the trading organisations; disposal of the money received from the realisation of the confiscated property; accounting of such funds.

In this way, statistical records are kept of the total volume of property confiscated by the state. However, the regulations do not provide for the maintenance of statistical records of disaggregated data according to the grounds for confiscation (within the framework of criminal, administrative proceedings, customs and tax legislation, etc.), the types of offences for which confiscation has been applied, the type of

property confiscated in the context of the provisions of recommendation 4 (laundered property, instrumentalities and means of crime, property of the corresponding value).

It was not possible to assess the completeness of the criminal statistics on the restitution to victims and confiscation of property by courts and the execution of court decisions in this part.

d) Mantaining statistics related to provision of legal assistance in criminal matters, extradition, criminal prosecution, transfer of convicted and mentally ill offenders for serving sentence and compulsory medical treatment and other cooperation in criminal matters is carried out by the GPO International Legal Cooperation Department (General Prosecutor's Order No.417 of 28.10.2017). According to the joint instruction of the GPO, SC, SSS, MIA, SCC, and National Guard (adopted in May 2021) on further improvement of work on sending requests to foreign countries for procedural actions in criminal cases and execution of similar requests of foreign countries, the MIA, SSS, SCC, National Guard, DCEC and BCI shall send quarterly data in this area to the GPO in the prescribed form.

Weighting and Conclusion

1783. In Uzbekistan, the mechanisms and responsible authorities for maintaining the statistics on matters relevant to the effectiveness and efficiency of their AML/CFT system are set out in the national legislation. However, the statistics are maintained not in full scope and cannot be considered comprehensive.

1784. **Recommendation 33 is rated Largely Compliant.**

Recommendation 34 – Guidance and Feedback

1785. In the 2010 MER, Uzbekistan was rated non-compliant with former R.25, as no guidelines or recommendations describing ML/FT methods and techniques were issued for institutions engaged in transactions with funds or other assets, and insufficient information on results of financial investigations conducted by the FIU was available to financial institutions. No special guidelines that could help financial institutions to more effectively perform their obligations, including description of new ML/TF trends and typologies, were issued.

Criterion 34.1

FIU

1786. The functions assigned to the DCEC include an extensive outreach and awareness raising work with a view to preventing economic and corruption-related offences, money laundering and financing of terrorism and proliferation (Par.10(9) of Regulation on DCEC No.UP-5446 dated 23.05.2018). For pursuing these objectives, the DCEC actively engages with mass media and general public and informs about results of its activity by holding workshops, briefings, press-conferences, roundtables and other outreach events (Par.11(9) of Regulation on DCEC No.UP-5446 dated 23.05.2018). For example, the DCEC has developed, in cooperation with the CB, the methodological guidance on comprehensive analysis of transactions by commercial banks for AML/CFT purposes (Letter No.23-23/161 dated May 12, 2020). The results of the sectoral risk assessment have been communicated to commercial banks by letter No. 23-23/416 of 08/10/2019.

1787. Chapter 6 "Reporting the Results of Suspicious Transaction Reports (Feedback)" of the Regulation on the Procedure of Reporting Information Related to AML/CFT/CPF, approved by PCM-402 of 29/06/2021, sets out FIU obligations to provide feedback to reporting entities on improving the quality of STRs. The Annexes to the Regulation contain an indicative STR submission scheme to facilitate understanding of this obligation by reporting entities.

1788. Launched on the DCEC official website is the Personal Account for providing feedback regarding particular laws and regulations, designated persons linked or suspected of being linked to terrorist activities, and quality of submitted STRs. The actual provision of feedback is done through workshops and meetings organised by the DCEC.

DNFBPs

1789. The ICR is the main AML/CFT guideline paper for DNFBPs. The ICRs are developed and adopted by the relevant oversight, registration and licensing authorities in cooperation with the DCEC, and where no such authorities are appointed – by the DCEC (AML/CFT Law, Art.6).

1790. Together with the DCEC, the supervisory authorities monitor and supervise the compliance of the reporting entities with the ICRs and develop guidelines to assist the DNFBPs. This work is carried out within the framework of the meetings with further submission of the minutes of these meetings. For example, by the Minutes № 2 from 06.02.2020, the Ministry of Finance has approved, placed on its website and sent to the organisations (DPMS, auditors, leasing and insurance companies) the Recommendations on the application of the results of the conducted NRA, the model questionnaire of the client. UzSAMA has repeatedly organised seminars for real estate institutions to raise awareness of their obligations to execute the ICR. The assessors have read the minutes of the workshops dated 07.01.2020, 09.03.2020, 02.09.2020, 28.04.20201. Similar seminars were conducted for the DPMS sector (22.01.2021), auditors (18.01.2020), and lotteries (10.06.2021). The DCEC, together with the supervisory authorities, conducts such activities on an ongoing basis.

1791. Despite disseminating guidelines, no activities aimed at providing feedback, including a better understanding of DNFBPs in identifying and reporting suspicious transactions, have been carried out.

FIs

1792. In Uzbekistan, the standard ICR for FI (that should be used for developing internal policies) set out the main AML/CFT obligations of the reporting entities. The ICR for banks and NBCI permit such institutions to include additional suspicious indicators based on the methodological guidelines issued by the CB (Par.50 of ICR No.2886 of 23.05.2017, and Par.37 of ICR No.2925 of 04.09.2017). The CB also conducts outreach by posting analytical materials and reviews, statistical data and interviews on its website (Art.69 of Law No.154-I on the CB dated 21.12.1995). Exchange members may apply methodological recommendations for the early detection of suspicious transactions developed by the Antimonopoly Committee in coordination with the FIU (point 30-1 of the PBC dated 06.11.2009 No. 2038). Operators and providers of postal service may implement indicators for early detection of suspicious transactions based on methodological recommendations developed by the Ministry of Finance in coordination with the FIU and having a recommendatory nature. Internal rules may establish additional criteria and indicators of suspicious transactions (para 40-1 of ICR No. 3061 of 28.08.2018).

1793. No information has been provided regarding other categories of fFIs (payment institutions sector, insurance, securities, leasing).

1794. The suspicious transaction identification and reporting criteria and procedures (as in case of DNFBPs) are set out in the legislation (CM's Resolution No.272 dated 12.10.2009). Information on on actual measures taken for clarifying the AML/CFT requirements, on established feedback mechanisms and on developed guidelines for FIs is set out in the response to core ussue 3.6 of the IO.3.

Weighting and Conclusion

1795. Uzbek legislation enables the competent authorities (DCEC) and supervisors to develop guidelines for FIs and DNFBPs and to provide feedback regarding compliance with the AML/CFT requirements. Besides that, there is no mechanism in place for providing specific recommendations regarding STR quality feedback.

1796. **Recommendation 34 is rated Largely Compliant.**

Recommendation 35 - Sanctions

1797. In the first round MER, Uzbekistan was rated partially compliant with former R.17. The assessors identified the following deficiencies: the possibility to apply a broad range of sanctions against all types of FIs (except for the banking sector) was not established; Art.179-3 of the CAO was not

applicable to all sectors; and sanctions provided for in the said article were not proportionate and dissuasive.

Criterion 35.1

1798. There is an administrative liability for violations of the AML/CFT/CPF legislation in the Republic of Uzbekistan.

1799. Pursuant to Article 179-3(1) of the CAO, the following intentional acts are an administrative offence: (i) violation of requirements for the reglamentation and implementation of internal controls; (ii) violation of requirements for the documentation and storage of CDD results; (iii) violation of requirements for the identification, assessment and documentation of risks; (iv) violation of requirements to refuse a transaction; (v) failure to submit, late submission or submission of non-compliant information to FIU on suspicious transactions; (vi) failure to comply with the legal requirement to freeze funds and other assets or suspend a transaction. These actions carry an administrative penalty in the form of a fine from 15 to 30 RSV (USD 345 to 690).[137]

1800. Part 2 of Article 179-3 of the CAO establishes administrative liability for i) violation by supervisory, licensing and registration bodies of the established procedure for monitoring and control over compliance with the ICRs; ii) wrongful request, receipt or disclosure of information constituting commercial, banking or other legally protected secrecies in connection with AML/CFT/CPF. These acts carry an administrative penalty in the form of a fine of 20 to 40 RSV (USD 460 to 920).

1801. The commission of offences under par. 1 and 2 of Article 179-3 of the CAO repeatedly within one year after the administrative penalty has been imposed shall be punishable with a fine under par. 3 of Article 179-3 from 30 to 50 RSV (from USD 690 to USD 1,150).

1802. If the violation of the AML/CFT/CPF legislation resulted in significant damage or material damage to the rights and legally protected interests of citizens or state and public interests, officials of legal entities may be held criminally liable for abuse of power (Articles 192-11 and 205 CC), exceeding power (Article 206 CC); official negligence (Article 207 CC); omission of authorities (Article 208 CC); forgery in office (Article 209 CC).

1803. The sanctions imposed by administrative and criminal law are dissuasive and proportionate (except those mentioned in Criterion 3.9 of R.3). Still, they only apply to natural persons, as legal persons' criminal and administrative liability has not been established in Uzbekistan.

1804. Civil law sanctions directly for non-compliance with AML/CFT legislation apply to a limited list of FIs and DNFBPs.

1805. At the same time, as noted in Recommendation 27, the state regulatory and supervisory authorities for FIs and DNFBPs (except for the CB) do not have sufficient powers to apply sanctions against legal entities that violate AML/CFT/CPF legislation.

1806. In case of non-compliance with the instructions, or in case of gross or systematic violations (two or more times a year) of AML/CFT/CPF legislation requirements, the CB is empowered to apply stricter sanctions, up to and including the revocation of the license.

1807. Failure by insurers to timely submit the list of compliance officers and AML/CFT reports to the Finance Ministry is punishable by administrative fine in amount of 0.05% of the minimum authorized capital (Regulation on imposition of punitive sanctions against insurers for breaches of the legislation dated 15.08.2008, Reg.No.1842).

1808. Breaches by the commodity exchange members of the requirements of the Uzbek Agro-Industrial Exchange Trade Regulations related to internal controls, customer identification and CDD measures identified by the DCEC or by the Commodity Exchange may result in prohibition from trading for up to 1 month until elimination of the identified breaches; or for up to 6 months in case of repeated

[137] Hereinafter all calculations are based on the exchange rate current as of 02.07.2021. In the first half of 2021, the average monthly nominal wage in Uzbekistan was 2,971,100 soums (about US$275). RSV on 02.07.2021 was 245,000 soums (about 23 USD).

breaches; or up to 1 year in case of multiple breaches, up to cancellation of the commodity exchange membership status.

1809. Concerning other FIs and DNFBPs, the basis for applying civil sanctions is a general rule prohibiting illegal activities (Article 53 of the Civil Code), as there are no direct norms on applying sanctions for violations of AML/CFT legislation.

1810. Breaches of the applicable legislation by notaries and lawyers entail suspension of licenses, up to license revocation (Art.19 of Law No.343-I on Notaries dated December 26, 1996; Art.14 of Law No.349-I on Lawyers dated December 27, 1996).

1811. Thus, the requirement to have a range of sanctions against legal entities for AML/CFT violations is not adequately enforced in the Republic of Uzbekistan, and their application is limited.

Criterion 35.2

1812. According to CAO Art.15, executive officers, including directors and senior managers, of legal entities are held liable for administrative offences covered by CAO Art.179-3 (on condition that they have breached a regulation whose enforcement is part of their official duties), and are also held liable for crimes against criminal breach of contracts of service.

Weighing and Conclusion

1813. In Uzbekistan, sanctions for violations of the AML/CFT requirements for legal persons are limited.

1814. **Recommendation 35 is rated Partially Complaint.**

Recommendation 36 – International Instruments

1815. In the 2010 MER, Uzbekistan was rated partially compliant with SR.1 and largely compliant with former R.35. The identified deficiencies included insufficient implementation of the Vienna and Palermo Conventions in terms of criminalization of possession or use of criminal proceeds as the ML element (CC Art. 243), and insufficient implementation of the International Convention for the Suppression of the Financing of Terrorism as regards criminalization of seizure of nuclear materials as well as unlawful acts against the safety of fixed platforms located on continental shelf. The revealed deficiencies were also related to insufficient international cooperation for combating crimes covered by the International Convention for the Suppression of the Financing of Terrorism and by the Vienna and Palermo Conventions.

Criterion 36.1

1816. The Republic of Uzbekistan has acceded to or ratified all mandatory conventions as provided for in the FATF Recommendations.

Table 36.1: Signed/ Ratified Conventions

Convention	Ratification
UN Convention against Transnational Organized Crime (Palermo Convention)	Oliy Majilis Resolution No.536-II of 30.08.2003 on Ratification of the United Nations Convention against Transnational Organized Crime
UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention)	Oliy Majilis Resolution No.32-I of 24.02.1995 on Accession to the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances
International Convention for the Suppression of the Financing of Terrorism (TF Convention)	Oliy Majilis Resolution No.225-II of 12.05.2001 on Ratification of the International Convention for the Suppression of the Financing of Terrorism
UN Convention against Corruption (Merida Convention)	Law No. ZRU-158 of 07.07.2008 on Accession of the Republic of Uzbekistan to the United Nations Convention against Corruption (New York, October 31, 2003)

Criterion 36.2

1817. Uzbekistan has criminalized most offences covered by the main Conventions (Palermo, Merida, Vienna and TF Conventions), including bribery, terrorist financing, money laundering and organized crime.

1818. Vienna Convention and TF Convention were ratified without any reservations. The assessed country has made the commitment to fulfill all MLA-related obligations (except for asset confiscation and recovery) set out in the conventions.

1819. The provisions of Merida Convention related definition of public officials and criminalization of the relevant acts are fully implemented in the Uzbek legislation. However, this definition is inconsistently applied in the regulations governing the activities of different types of financial institutions (see Criterion 12.1).

1820. Uzbekistan has ratified Palermo Convention with the reservation stating that the provisions of Article 10 that require to hold legal entities criminally or administratively liable for participation in criminal activities are inapplicable due to the specificities of the national legislation (see Criterion 3.10). Since implementation of the said Article is the mandatory requirement under the FATF Recommendations, the aforementioned reservation has a significant impact that prevents this criterion from being fully met by the assessed country.

1821. A shortcoming in implementation of the requirements of the main conventions is that the Uzbek legislation lacks the provisions for establishing different types of confiscation. It is necessary to provide confiscation as an adequate measures for the seizure of criminal assets, which all the major conventions contain. However, Oliy Majilis Resolution No.536-II of 30.08.2003 on Ratification of Palermo Convention states that national legislation lacks the relevant provisions and such provisions cannot be adopted in respect of Art.2 (g) of the Convention. In this context, the applied measures are limited to transfer of illegally obtained property back to its legitimate owners (restitution) and appropriation of seized property to the state budget on a case-by-case basis. Furthermore, the presented information and case studies contained the examples of confiscation only in the situations where the criminal property was officially recognized and accepted as material evidence. However, the Uzbek legislation does not provide for confiscation in the situations when criminal proceeds are intangible (e.g. funds in a bank account), or when criminal property is not recognized and accepted as material evidence under CPC Art.203 (e.g. when criminal proceeds are fully spent, and property of corresponding value cannot be confiscated, unless it is the instrumentalities of crime under CPC Art.284).

1822. The requirements of the main conventions related to access by the LEAs to financial information are fully implemented in the national legislation. On 28.06.2021, the amendments were introduced into Uzbek Law No.530-II on Banking Secrecy dated 30.08.2003 that enabled to obtain information in the course of any criminal proceedings and criminal intelligence gathering and detective operations (Art.9) and to provide such information to foreign competent authorities. Article 5 of Law No.530-II states that exchange of relevant information with foreign competent authorities in a manner established by the national legislation and international treaties and agreement signed by the Republic of Uzbekistan does not constitute unauthorized disclosure of bank secrets.

1823. The criminal procedure legislation establishes the general procedure for conducting searches and seizing documents (CPC Chapter 20). The legislation lacks special provisions governing seizure of documents containing information deemed a bank secret, but, at the same time, imposes no limitations and restrictions in respect of this process. The revised Articles 5 and 9 of Law No.530-II allow investigators and inquirers to obtain information constituting bank secrets from banks and share this information with foreign competent authorities. According to these provisions, prosecutors are also involved in the process of exchange of relevant documents, which is quite important from the MLA perspective. The overall interpretation of the aforementioned legislative provisions allows for making a conclusion that they enable seizure and exchange of documents containing bank secrets for the MLA purposes.

Weighting and Conclusion

1824. Uzbekistan has become a party to all mandatory conventions (Palermo, Merida, Vienna and the International Convention for the Suppression of the Financing of Terrorism), and most provisions of these conventions are implemented in the national legislation. The confiscation regime requires improvement, as it is limited to restitution and seizure of material evidence only. Besides that, the deficiencies in R.12 related to requirements for financial institutions to identify politically exposed persons (PEPs) impact the full implementation of Merida Convention.

1825. **Recommendation 36 is rated Largely Complaint.**

Recommendation 37 – Mutual Legal Assistance

1826. In the 2010 MER, Uzbekistan was rated largely compliant with former R.36 and partially compliant with SR.5. The deficiencies identified in implementation of R.35 included absence of a mechanism to determine the best venue for the prosecution of defendants. As for SR.5, it was noted that issues related to sharing confiscated property with other countries when confiscation is directly or indirectly a result of coordinated law enforcement actions were not regulated by the Uzbek legislation.

Criterion 37.1

1827. The Uzbek national legislation provides the necessary legal basis for rendering and receiving MLA. The relevant provisions are contained in a separate Chapter (Chapter 65, Article 592-598) of the CPC.

1828. The Uzbek LEAs and judicial authorities may seek legal assistance in criminal matters from foreign competent authorities under the relevant international treaties/ agreements and also based on the principle of reciprocity (CPC Art.592). According to the information provided by the assessed country, Uzbekistan is a party to 5 international conventions, 6 regional treaties and 32 bilateral agreements, which enables it to receive and provide legal assistance.

Criterion 37.2

1829. As provided for in Article 592 of the CPC, the SC, the GPO, the MIA and the SSS are designated as the central bodies responsible for MLA. Their mandates are described in Table 37.2. According to Par.2 of the joint Directive issued by the GPO, MIA, SSS, SC, National Guard and SCC "On further improvement in requests to foreign countries for criminal proceedings and the execution of similar requests from foreign countries" the GPO is defined as the national MLA coordinating body.

Table 37.1

Agency	Mandate
Supreme Court	Issues related to criminal prosecutions by courts of general jurisdictions
Ministry of Internal Affairs State Security Service	Procedural actions that do not require court order or prosecutor's consent (authorization)
General Prosecutor's Office	All other issues

1830. In the GPO, the internal case management procedures, including MLA request processing procedures, are set out in the document management and execution monitoring instructions (General Prosecutor's Orders No.225 dated 25.12.2020 and No.176 dated 15.12.2017 (both documents are confidential) that regulate the processes for prioritization and timely execution of MLA requests and for monitoring the document flows. General Prosecutor's Order No.225 also governs the electronic document management procedures that enhance the effectiveness of cooperation. The provided information shows that the GPO, being the central body responsible for mutual legal assistance in a wide range of criminal matters, pays a great deal of attention to regulation of the case management systems and procedures.

1831. Other LEAs also have their own internal regulations. In particular, the SSS adopted the internal regulation dated 31.12.2018 for arranging and implementing the internal monitoring system. According to this regulation, the SSS international cooperation department is responsible for monitoring and pursuing the coordinated policy in the area of international cooperation with foreign

counterparts, while the document management department and the senior leadership of the SSS monitor timely execution of requests. The MIA has also established the department responsible for overseeing execution of orders and documents that also monitors timely execution of MLA requests.

1832. Apart from the internal regulations of different agencies, a number of national-wide regulations have been adopted that apply to all competent authorities. In particular, on 29.06.2021, the CM issued Resolution No.402 that adopted the Regulation on International AML/CFT/CPF Cooperation. According to Par.33 of this Regulation, upon receipt of MLA requests, the competent authorities shall determine the process for their execution, including priority and timelines. Besides that, Par.4 of the joint Directive obliges the competent authorities to rapidly execute foreign requests related to corruption, money laundering, terrorist financing and proliferation financing as well as requests related to identification, tracing, seizure, confiscation and recovery of assets.

Criterion 37.3

1833. According to CPC Art.595, an MLA request is denied if it contradicts the legislation of Uzbekistan or if its execution may infringe sovereignty or security of the Republic of Uzbekistan. In such situation, the received request is returned with explanation of reasons that prevents its execution. Otherwise, the Uzbek legislation contains no unreasonable or unduly restrictive conditions for the provision of mutual legal assistance.

Criterion 37.4

a) The Uzbek legislation does not prohibit execution of MLA requests that involve fiscal matters.

b) The amended Art.5 and Atr.9 of Law No.530-II allow the competent authorities to receive information constituting bank secrets and share such information in the process of mutual legal assistance.

1834. There are no prohibitions and restriction in the Uzbek legislation that could prevent execution of MLA requests that seek for information constituting bank secrets. Furthermore, Resolution No.402 explicitly states that the central bodies may not refer to bank secrecy as the grounds for refusal to provide information or execute requests.

Criterion 37.5

1835. A number of confidentiality related provisions have been added into the Uzbek legislation in recent years. In particular, Par.38 of the International AML/CFT/CPF Cooperation Regulation obliges all competent authorities to maintain confidentiality of MLA request and information contained therein as well as the information provided by them.

1836. Apart from that, Par.9 of the joint Directive proscribes all officers of judicial, prosecution, investigation and inquiry authorities to maintain confidentiality in the course of processing and executing MLA documents.

1837. CPC Art.353 authorized investigators to recognize information contained in criminal files as confidential. CC Art.239 established liability for unauthorized disclosure of preliminary (pre-trial) investigation information.

Criterion 37.6

1838. The Uzbek legislation does contain provisions that make dual criminality a special condition for rendering the requested mutual legal assistance. Notably, Par.3 of the joint Directive stipulates that in case of receipt of a request from a foreign competent authority related to actions that are not criminalized by the Uzbek law, the competent authorities shall execute such request to the extent that the sought assistance can be provided without application of coercive actions.

Criterion 37.7

1839. The Uzbek legislation contains no provisions indicating that the lack of dual criminality may constitute the grounds for refusal to provide mutual legal assistance.

1840. However, CPC Art.595 provides that a request may be denied if contradicts the legislation of Uzbekistan, and according to the same Article, the CPC provisions are applied in the course of

execution of requests. Since the CPC sets out specific conditions for investigative actions that limit civil rights (e.g. search and seizure) under the instituted criminal proceedings (i.e. there should be a sufficient preliminary evidence of a committed criminal offence), technically, dual criminality is a mandatory condition for rendering such kind of mutual legal assistance. Such approach in common in most countries across the globe, including the FATF and EAG members.

1841. Subparagraph 2 of paragraph 3 of Joint Directive No. 35/28-21/30k/4/01-02/17-30/6 of 04.05.2021 instructs the competent authorities when assessing whether the unlawful act for which extradition is sought constitutes an offence under Uzbek law, to assume that the deficiencies in the name and description of the individual elements of the crime do not have significance.

Criterion 37.8

a) According to CPC Art.595, all provisions of the national criminal procedure legislation are applied to execution of requests related to procedural actions. Therefore, any mechanisms provided for in the criminal procedure legislation consistent with Recommendation 31 may be used for executing MLA requests.

b) Competent authorities may also use any other means of information gathering not prohibited by law, including diagonal communication and open data sources.

Weighting and Conclusion

1842. **Recommendation 37 is rated Compliant.**

Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation

1843. In the 2010 MER, Uzbekistan was rated partially compliant with former R.38. The legislation did not provide for confiscation of property of corresponding value, and shortcomings in criminalization of ML limited potential application of confiscation mechanism. Uzbekistan did not consider sharing confiscated assets with foreign competent authorities that contributed to confiscation of such assets, and did not provide the MLA related statistics.

Criterion 38.1

1844. MLA on detection, freezing, seizure and confiscation are carried out in accordance with the provisions of the CPC and ratified international conventions, treaties and agreements.

1845. According to CPC Art.595, a court, prosecutor, investigator and inquirer shall execute a request for procedural actions received from a relevant foreign competent authority and submitted to them in the established manner. When executing such requests, they use the procedural legislation of Uzbekistan or the legislation of a requested country unless it contradicts the legislation of the Republic of Uzbekistan. Meanwhile, the country's national legislation (Art. 9 of Law No. 530-II) ensures effective asset tracing, including obtaining bank secrecy and other sensitive information by requesting it from other public bodies, including the FIU (see R.4 and 31 for more details).

1846. Uzbekistan has designated the central competent authorities empowered to execute incoming requests for identification, seizure, freezing and confiscation of assets: the GPO, the MIA and the SSS. According to Art. 592 of the CPC, the MIA and the SSS are central for the execution of requests unless such execution requires a judicial decision or the prosecutor's authorisation. Otherwise, the request for MLA is sent through the GPO.

a) According to art. 211, para 5, of the CPC, money and other valuables obtained by criminal means and laundered property may be confiscated. Property that is the object of a crime is confiscated based on art. 284 of the CPC.

b) Money, things and other valuables acquired with the proceeds of crime, as well as money, things and other valuables obtained from the sale of criminal property, shall be confiscated pursuant to Article 285 of the CPC.

c) and d) Instrumentalities used to commit any offence, including ML and TF, as well as those intended for the preparation or commission of such crimes, are confiscated under Article 211 of the CPC.

e) Property of corresponding value may be confiscated based on Article 284 of the CPC.

1847. The competent authority for freezing assets within the FIU competence under Decree No. UP-5446 of 23.05.2018 is the DCEC, including on requests from foreign FIUs.

Criterion 38.2

1848. The GPO is authorised as a competent authority to liaise within the MLA requests on non-conviction based confiscation in the above cases.

1849. However, it should be noted that the possibility of actually executing a foreign state's request for non-conviction-based confiscation is limited.

1850. Based on the legislation provided by the country, the enforcement of foreign judgments in non-conviction-based confiscation depends on the legal act under which the MLA request is processed. Where enforcement of a non-conviction-based confiscation judgment is allowed under an international treaty on MLA (convention, treaty, agreement, etc.) ratified by Uzbekistan, it appears that such a confiscation judgment may be enforced.

1851. For example, the 2002 CIS Chisinau Convention on Mutual Legal Assistance in Criminal, Civil and Family Matters (Article 58) provides that court decisions (not only sentences) on confiscation are enforceable by the contracting parties. However, only the party requesting the MLA may review the confiscation decision. The law of the requested party determines only the procedure of confiscation. The requested party is bound by the findings of fact to the extent that they are set out in the sentence or other judgement rendered by the requesting MLA or to the extent that the sentence or other judgement is based on those findings.

1852. According to Article 2, para 3, of Law No. ZRU-518 of 06.02.2019 "On International Treaties of the Republic of Uzbekistan", in cases where an international treaty of the Republic of Uzbekistan establishes rules other than those stipulated by the legislation of the Republic of Uzbekistan, the rules of the international treaty shall apply.

1853. Based on the above, non-conviction-based confiscation MLA may be granted in such a case.

1854. However, in cases where a treaty does not permit non-conviction-based confiscation, or the MLA request is executed on the principle of reciprocity (in the absence of a treaty), such confiscation may be executed in limited cases.

1855. According to article 595, paras 4 and 7, of the CPC, the competent authorities of Uzbekistan execute requests for MLA under the rules of the Code. The rules of procedure of the foreign state may be applied under the request of the competent authority of a foreign state if this does not run counter to Uzbek law. If the MLA request is inconsistent with Uzbek law, it must be returned without being executed.

1856. Pursuant to para 17 of annex 2 to CM Resolution No. 402 of 29.06.2021, requests from the competent authorities of foreign States for the recognition and enforcement of a judgement or ruling of a foreign court concerning confiscation of property obtained through the commission of an offence which is located in Uzbekistan are executed in accordance with the law.

1857. Uzbekistan provides for non-conviction-based confiscation in only two cases:

- Confiscation, upon the termination of the criminal case, of instrumentalities of crime belonging to the suspect or the accused that are recognised as physical evidence in the case (Art. 211 of CPC).
- Confiscation (collection) by the court of money and other property from criminal activities within the civil judicial procedure if related to ML or TF criminal cases were terminated;[138]
- Confiscation (collection) by the court of the equivalent value of the property that was the object of the crime in the terminated criminal case, if such property itself is not found (Art. 284 of CPC).

[138] Resolution No. 2174 of the Ministry of Justice of 29.12.2010, Order No. 129 of the Prosecutor General of 22.12.2016

1858. A decision to discontinue criminal proceedings in respect of the grounds for non-conviction-based confiscation mentioned in the interpretive note to Recommendation 38 (when the offender is dead, has escaped, is not available or not identified) under the CPC is made only when the person has died, otherwise, the case is suspended. Accordingly, the application of non-conviction based confiscation in the above-mentioned situations is only possible in case of death of the person, and, moreover, it's possible in cases when a criminal proceeding is discontinued due to the expiration of limits for bringing a person to justice or an amnesty act, or due to the exemption of a person from liability on account of active repentance (see note to article 155-3 of the CC, Criterion 5.6).

1859. The Uzbek authorities stated that non-conviction based confiscation is unenforceable, as it contradicts the fundamental principles of the domestic law, since according to Article 26 of the Constitution of Uzbekistan any person accused of committing a crime shall be considered innocent until his/her guilt is proven in accordance with the procedure stipulated by the law in open court proceedings with provision of all means to defend himself/herself. However, this statement cannot be accepted, as non-conviction based confiscation does not require a conviction. In addition, as noted above, such confiscation may be applied to certain types of property in the above-mentioned circumstances.

Criterion 38.3

a) Uzbekistan has acceded to most international MLA treaties related to seizure and confiscation actions, including Vienna, Merida, Palermo UN Conventions and International Convention for the Suppression of the Financing of Terrorism, Chisinau Convention of the CIS Member States. Besides that, Uzbekistan has signed a number (more than 10) of bilateral MLA agreements that establish the cooperation and coordination mechanisms for identification, tracing, seizure and confiscation of assets. Such agreements are signed by Uzbekistan with most neighbouring countries (Kazakhstan, Turkmenistan and Kyrgyzstan) as well as with its major economic partners, including the EAG member countries (China and India). However, most of these treaties do not contain provisions on the enforcement of confiscation judgments. Thus, the MLA issues on the enforcement of confiscation judgments with countries with concluded international treaties, as well as with all other countries (except for cooperation within the framework of the above-mentioned conventions) is based on the principle of reciprocity in accordance with the rules of the Uzbekistani CPC.

b) Mechanisms for the management (recording, storage, etc.) and disposal of frozen, seized and confiscated property are regulated in the Regulation on the Procedure for Seizure, Sale or Destruction of Property Subject to Transfer to State Revenue, approved by CM Decision No. 200 of 15.07.2009. Considering that when executing MLA requests, in cases where international treaties do not regulate the rules for dealing with the requested actions, the Republic of Uzbekistan applies domestic legislation, the procedure for managing and disposing of frozen, seized or confiscated property based on MLA requests is the same.

Order and conditions of storage of seized and confiscated property in enforced execution of judicial acts and acts of other authorities are determined by the Regulation on order and conditions of storage of seized and confiscated property in enforced execution of judicial acts and acts of other authorities approved by Decree of Cabinet of Ministers of 08.05.2009 No. 132.

The procedure of seizure (acceptance), registration, storage, transfer, return, disposal and destruction of material evidence, material values and other property in the process of inquiries and pre-trial and court investigations is determined in accordance with the provisions of Interagency Resolution No.2174 dated 29.12.2010.

According to Para.17 of CM Resolution No. 402 of 29.06.2021, confiscation requests are executed by competent authorities in line with the national legislation and, therefore, all aforementioned regulations apply to execution of such requests.

Criterion 38.4

1860. CM Resolution No. 402 of 29.06.2021 allows for sharing confiscated assets. Par.20 of the said Resolution permits LEAs to enter into agreements or otherwise agree, on a case-by-case basis, to share confiscated funds or other assets or income received from sale of confiscated assets.

1861. In relations with countries that have ratified the CIS Chisinau Convention of 2002, the possibility of sharing confiscated property is provided for in Article 58 of the Convention, which states that in each case, the requesting and requested parties shall agree on the sharing of property received by the requested party in the execution of the confiscation order in accordance with the Convention.

Weighting and Conclusion

1862. In Uzbekistan, the possibility of actually enforcing a foreign request for non-conviction-based confiscation is limited.

1863. Enforcement of confiscation judgments may be based on a limited number of international treaties, as well as on the principle of reciprocity.

1864. **Recommendation 38 is rated Largely Compliant.**

Recommendation 39 – Extradition

1865. In 2010 MER, Uzbekistan was rated compliant with former R.39.

Criterion 39.1

a) The extradition process is governed by a separate chapter of the Criminal Procedure Code (Chapter 64). According to CPC Art.601 the General Prosecutor's Office is the designated body authorized to consider extradition requests. This Article also sets out the grounds for extradition if one of the following conditions is met:

- If the request is made for a person who has not yet been convicted, he or she may be extradited if the CC provides for a sentence of imprisonment of at least 1 year or more severe punishment for the act committed. ML/TF offences fully satisfy this ground, as the minimum sentence for ML is 5 years (Article 243 of the CC) and for TF is 8 years (Article 155-3 of the CC);
- If the person who is the subject of the extradition request has been sentenced to imprisonment, this should not be less than six months. ML/TF offences also meet this criterion, and the person convicted of these offences is subject to extradition;
- In cases where temporary extradition is required (e.g. the person has already been convicted in Uzbekistan and is serving a sentence), the foreign State making the request must ensure that the person who is the subject of the request will only be prosecuted for the offence referred to in the request and that a number of guarantees in terms of his/her constitutional rights will be observed.

Thus, in Uzbekistan, ML and TF may constitute the grounds for extradition of persons to foreign states subject to reasonable conditions and guarantees of their rights.

b) The GPO has issued the Instruction governing the document processing and case management processes that sets out clear procedures and establishes the system for monitoring timely execution of extradition requests.

c) The grounds for rejection of extradition requests are listed in the CPC Art.603. In particular, a person may not be extradited if: he/she is the citizen of the Republic of Uzbekistan; the criminal offence has been committed in the territory of Uzbekistan; a sought person has been effectively convicted in Uzbekistan for the same offence; an action underpinning the extradition request is not criminalized in Uzbekistan; the statute of limitations has expired or there are other legal grounds that exclude criminal prosecution; criminal proceedings have been instituted against the sought person in Uzbekistan; a person whose extradition is requested has been granted asylum in Uzbekistan.

Extradition of a person for serving a sentence may also be refused if there are reasonable grounds to believe that that the convicted person was denied the sufficient opportunity to defend himself/herself.

Thus, the main grounds for extradition listed above allow for making a conclusion that the conditions

for denying extradition set out in the Uzbek legislation are reasonable.

Criterion 39.2

a) CPC Art.603 forbids extradition of the citizens of Uzbekistan.

b) CC Art.12 and CPC Art.598 allow for criminal prosecution of the Uzbek citizens who have committed criminal offences broad. According to CPC Art.598, the General Prosecutor's Office is designated as the agency authorized to consider extradition requests and coordinate further measures and actions in such situations.

Criterion 39.3

1866. According to the requirements set forth in the CPC, lack of dual criminality constitutes the grounds for denial of extradition. Apart from this, the criminal procedure legislation sets no additional conditions related to gravity of committed crimes, with the only exception that accused persons shall not face death penalty abroad. According to sub-para 2 of para 3 of Joint Directive No. 35/28-21/30k/4/01-02/17-30/6 of 04.05.2021 when assessing the MLA request, it should be presumed that the deficiencies in the name and description of the individual elements of the crime do not have significance. According to article 601 of the CPC, extradition may take place if the act is punishable under the CC of Uzbekistan by at least one year's imprisonment or a more severe penalty. Thus the criterion for extradition is not the qualification of the act but its punishability under Uzbekistan's CC.

1867. Similar provisions are contained in some international treaties ratified by Uzbekistan. In particular, according to para 4 of Article 66 of the 2002 Chisinau Convention of the CIS Member States, when deciding whether the act for which extradition is requested is a criminal offence under the domestic law of the requested and requesting parties, differences in the description of individual features of the crime and the terminology used are irrelevant.

Criterion 39.4

1868. The law of criminal procedure does not provide for procedures for simplified extradition; the relevant mechanisms are established in the international treaties of Uzbekistan with other States. Simplified extradition procedures are provided for in Uzbekistan's bilateral international treaties, including Turkey (art. 12) and the Republic of Korea (art. 10). Such procedures apply, for example, where a person voluntarily agrees to be extradited.

Weighting and Conclusion

1869. **Recommendation 39 is rated Compliant.**

Recommendation 40 – Other Forms of International Cooperation

1870. In the 2010 MER, Uzbekistan was rated partially compliant with former R.40 and largely compliant with SR.V. The identified deficiencies were related to lack of international AML/CFT cooperation by law enforcement and supervisory authorities, insufficient international cooperation by the FIU and absence of effective mechanisms and channels for sharing information with foreign counterparts.

Criterion 40.1

1871. The Uzbek national legislation contains the provisions that enable other forms international cooperation, including establishment and coordination of contacts with foreign counterparts.

1872. The relevant provisions are set out in Article 7 of RU Law No.ZRU-518 of 06.02.2019 on International Treaties of the Republic of Uzbekistan that defines the powers of particular government authorities to enter into international treaties and agreements.

1873. Besides that, Art.22(1) of AML/CFT Law No.660-II dated 26.08.2004 also provides the opportunities for such cooperation.

Criterion 40.2

a) The Uzbek competent authorities has a sufficient legal basis for establishing contacts with foreign counterparts and entering into international agreements, which is set out both in the national legislation (see criterion 40.1) and international legal instruments.

International agreements are signed by the Uzbek competent authorities at the government level as well as at the level of individual agencies, including LEAs (GPO, MIA, SSS, SCC, etc). This possibility is provided in Article 7 of the Law on International Treaties No. ZRU-518 of 06.02.2019, under which state government authorities conclude inter-institutional international treaties within the limits of their competence. According to Article 33 of above Law international treaties of the Republic of Uzbekistan are subject to strict and binding application by the Republic of Uzbekistan.

In addition, the NLAs governing the relevant authorities also contain provisions that provide a legal basis for international cooperation, inter alia:

- GPO - art. 52 of Law No. 257-II of 29.08.2001 "On Prosecutor's Office";
- DCEC - art. 7(11) of the Regulation on the DCEC, approved by Presidential Decree No. UP-5446 of 23.05.2018;
- MIA – art. 45 of the Law of 16.09.2016 ZRU-407 "On Internal Affairs Bodies";
- SSS – art. 45 of the Law of 05.04.2018 ZRU -471 "On State Security Service";
- SCC - art. 35 of the Law of 29.08.1997 No. 472-I "On the State Customs Service";
- STC - art. 16 of the Law of 29.08.1997 No. 474-I "On the State Tax Service";
- Central Bank - art. 54 of the Law of 21.12.1995 No. 154-I "On the Central Bank";
- Ministry of Justice – sub-para 17, para 12 of the Regulation on the Ministry of Justice approved by Presidential Decree No PP-3666 of 13.04.2018;
- Ministry of Finance – sub-para 28, para 11 of the Regulation on the Ministry of Finance, approved by Presidential Decree No. PP-2847 of 18.03.2017.

b) The Uzbek competent authorities can cooperate directly with the government authorities of foreign countries as well as with international and regional organizations and use the most efficient means.

c) The Uzbek competent authorities use not only the traditional communication channels, including the government courier service, regular mail, diplomatic mail, etc.

For operational cooperation, contact persons representing the LEAs at diplomatic missions may be used. In liaison with individual competent authorities (usually in case of inter-agency agreements), the appointment of contact persons from the relevant authorities is used.

Appropriate secure communication channels can be used as gateways mechanisms for information exchange through regional specialised structures: the CIS Anti-Terrorist Centre (CIS ATC), the CIS Office for Coordination of Combating Organised Crime and Other Dangerous Types of Crime (CIS BKBOP), the SCO Regional Anti-Terrorist Structure (SCO RATS), the Central Asian Regional Information and Coordination Centre for Combating Illicit Trafficking of Narcotic Drugs, Psychotropic Substances and their Precursors (CARICC).

The GPO interacts through ARIN-WCP, a CARIN-type regional group.

The DCEC uses relevant communication channels within the framework of Egmont Group membership (Egmont Secure Web).

The LEAs also uses relevant Interpol channels.

d) Certain provisions of the national legislation establish the deadlines for processing documents in the process of international cooperation in other formats. In particular, Par.33 of CM Resolution No.402 of 29.06.2021 prescribes the competent authorities to set the priorities and timelines for execution of international requests. Besides that, the GPO and DCEC has the regulatory procedures in place for prioritization of AML/CFT requests, and other government agencies also have the established deadlines for executions of requests received via the FIU.

e) Art.19 of AML/CFT Law No.660-II of 26.08.2004 sets out the general requirements for maintaining confidentiality by the FIU officers who process information constituting various secrets (bank, commercial, etc. secrets). Certain provisions of international treaties, including the Egmont Group regulations, are also applied.

The national legislation requires the government authorities to ensure protection and security of information resources and information systems, including information related to the public sector and other confidential information (Art.20 of Law on Information Technologies No.560-II dated 11.12.2003; Presidential Resolution No.PP-1572 dated 08.07.2011; CM Resolution No.295 dated 16.10.2015).

Set out in Paragraph 38 of Resolution No.402 of 29.06.2021 are the general requirements for all government authorities to maintain confidentiality in the process of international cooperation, and Par.42 of the said Resolution allows for using the secure communication channels for this purposes.

Besides that, most competent authorities, including the LEAs (MIA, SSS, SCC), have the internal information security policies that include measures for maintaining confidentiality of the processed documents. In particular, the Instruction governing the document processing and case management processes in the prosecution authorities forbids to release official documents to third parties and to use such documents, including information contained in incoming international requests, for purposes other than needed for discharging the official duties.

Criterion 40.3

1874. The Uzbek competent authorities are empowered to enter into international treaties and agreements required for discharging their functions and to establish direct contacts based on the principle of reciprocity.

Criterion 40.4

1875. In the course of cooperation with the Egmont Group members, Uzbekistan adheres to the principles of providing feedback to its counterparts.

1876. CM Resolution No.402 of 29.06.2021 obliges the government authorities to provide feedback regarding executed international requests. This requirement applies to all competent authorities, and the DCEC has issued a number of internal orders emphasizing the importance of compliance with this requirement.

Criterion 40.5

a) According to Art.76 of the Tax Code, transmission of information to foreign fiscal and other government authorities does not constitute the disclosure of bank secrets. The legislation does not provide for restrictions on the execution of requests involving fiscal matters.

b) Although national legislation contains a significant number of sectoral rules requiring regulated entities to keep financial information confidential, this is not a legal impediment to providing such information to the FIU and LEAs by virtue of their powers, nor does it prevent the transfer of such information to foreign competent authorities.

c) The Uzbek legislation does not impose limitations or restriction for execution of incoming requests. However, CPC Art.353 authorizes investigators to sworn people to secrecy requiring them not to disclose the preliminary investigation information, but it is permissible to make them public with the investigator's permission so that making them public does not violate the interests of the preliminary investigation and the rights and legitimate interests of the participants in the criminal proceedings. Under the general rule laid down in the CPC, this restriction applies until a final decision has been taken on the case.

d) The Uzbek legislation does not place any restrictive condition on execution of requests on the grounds that the legal system of a requesting country is different from that of Uzbekistan. Furthermore, para 38 of CM Resolution No. 402 expressly stipulates that difference in the status of a foreign competent authority may not be used as the grounds for rejecting a request.

Criterion 40.6

1877. Uzbekistan has acceded to a number of international and regional treaties governing the process of the use of information received in the course of international cooperation. The relevant provisions of these treaties are implemented in the Uzbek national legislation. In particular, Art.68 of the Law on the CB authorizes the CB to disclose information received from a foreign country only upon prior authorization and for the purposes for which such authorization has been obtained.

1878. Besides that, para 40 of CM Resolution No.402 provides that information received in the course of international cooperation shall be used only for the purposes set forth in requests or for responding to incoming requests. Such information may be disseminated to other government agencies for administrative or criminal proceedings and/or prosecutions only upon prior authorization of foreign competent authorities that have provided this information.

Criterion 40.7

1879. Under paras. 38-40 of Annex 2 to CM Resolution No. 402 of 29.06.2021, the competent state authorities of the Republic of Uzbekistan are obliged in accordance with the established procedure to ensure confidentiality of requests and information contained in them as well as information provided. If it is not possible to ensure confidentiality of information, the competent authority of the foreign state that sent the request must be immediately notified. Information obtained in international cooperation shall be used only for the purposes specified in the request or the response to such a request. The transfer of this information to public authorities or third parties or the use of this information for administrative and criminal proceedings shall only take place with the authorisation of the competent authority of the foreign state.

1880. According to para 37, annex 2 of CM Resolution No. 402 allows competent authorities to refuse to execute an international request, if a requesting party does not guarantee confidentiality and protection of provided information. Besides that, the international obligations undertaken by Uzbekistan allow it to make such decisions in particular circumstances.

Criterion 40.8

1881. The Uzbek legislation permits to conduct investigations at request of foreign competent authorities and share with them the obtained information as well as to exchange such information in the process of international cooperation conducted in other forms. Such provisions are set out, *inter alia*, in Art.15 of Law No.ZRU-344 on OIA dated 25.12.2012 and in Art.45 of Law No.ZRU-407 on Internal Affairs Bodies dated 16.09.2016.

Criterion 40.9

1882. Uzbekistan has an adequate legal basis for providing international cooperation, and the DCEC has all necessary powers to provide international AML/CFT/CPF cooperation (Art.9 (14, 15, 16) of the AML/CFT Law, and Par.11(7) of the Regulation on DCEC).

1883. As a member of the Egmont Group, the DCEC may share information with any other Egmont Group member FIUs based on the principle of reciprocity and in line with the Egmont Charter and Principles of Information Exchange.

1884. The DCEC has signed 22 cooperation agreements with foreign competent authorities.

Criterion 40.10

1885. As a member of the Egmont Group, the DCEC is obliged to provide feedback as required by Par.19 of the Egmont Principles of Information Exchange. The issues related to provision of feedback on the use and usefulness of received information from foreign counterparts are governed by the memoranda and agreements signed by the DCEC with foreign FIUs. Art. 22(2) of the AML/CFT Law empowers the DCEC to send information requests to foreign competent authorities and to respond to requests received from foreign competent authorities.

1886. There are no legal provisions to prevent the DCEC from providing feedback, upon request or whenever possible, to its counterparts on the use of the information provided by them, as well as on the outcomes of the analysis conducted on the basis of such information.

Criterion 40.11

a) and b) According to para 2 of Presidential Decree No.5446 dated 23.05.2018, cooperation with competent authorities of foreign countries and international specialist or other organizations with a view to combating economic crime, corruption, money laundering, terrorist and proliferation financing is one of the priorities of the DCEC.

The AML/CFT Law imposes no restrictions on sharing information by the designated AML/CFT agency. According to the Regulation of the DCEC (Par.11(7)), the DCEC cooperates and exchanges information, under the international treaties and agreement signed by Uzbekistan or on the basis of reciprocity, with foreign competent authorities and international organizations for combating economic crime, corruption, money laundering, terrorist and proliferation financing.

Criterion 40.12

1887. The Regulation on the Procedure for Conducting International Cooperation in AML/CFT/CPF sphere, approved by the Resolution of the CM No. 402 of 29.06.2021, regulates the issues of international cooperation of supervisory bodies (sub-paras.8, 9, para 4 item 38). Financial supervisory authorities have legal grounds to ensure cooperation with relevant foreign supervisory authorities and international organisations on their activities, including AML/CFT. The supervisory authorities of Uzbekistan must not refuse to execute a request, referring to differences in the status of the competent authority of a foreign state.

Criterion 40.13

1888. According to sub-para 1, para 8 of the Regulation on the Procedure for International Cooperation in the Field of AML/CFT/CPF, approved by the Resolution of the CM, supervisory authorities may exchange information or documents, which are available to supervisory authorities or which they may receive within their competence. The relevant NLAs for the CB, the Ministry of Finance, the Insurance Market Development Agency under the Ministry of Finance, the MITCD, and the Antimonopoly Committee provide information exchange within the scope of competence, without explicit reference to the possibility of exchanging confidential information.

Criterion 40.14

1889. In accordance with points 8, 9 of the CM Regulation No. 402 of 29.06.2021, international cooperation of supervisory bodies with the relevant supervisory bodies of foreign countries and international organisations shall be conducted, inter alia, in the following areas:

- Regulatory information (sub-para 5 para 9 of the Regulation);
- Prudential information (sub-paras 2, 3 p.9);
- AML/CFT information (sub-paras 4, 6 para 9).

1890. The CB has developed and approved by Resolution No. 23/10 of 10.10.2020 of the Management Board the Procedure for information exchange with international organisations, central banks and other foreign banking supervisory bodies in the field of AML/CFT, in accordance with which information is exchanged with foreign banking supervisory bodies.

Criterion 40.15

1891. Sub-para 3 of para 8 of the CM Regulation No 402 of 29.06.2021, established as directions of international cooperation of supervisory bodies with relevant foreign supervisory authorities and international organisations inspections (inquiries) of financial institutions on international request in the manner prescribed by law.

1892. For enabling the Central Bank to perform its supervisory functions, Article 61 of Law No.ZRU-582 of 11.11.2019 empowers the Central Bank to:

- Conduct inspections (audits) of credit institutions and associated entities, payment service providers, payment system operators, foreign currency exchanges, credit bureaus, entities carrying out transactions and providing services outsourced by banks, and entities that are subject to consolidated supervision.

1893. According to the Par.16 of the Regulation on the Antimonopoly Committee approved by Resolution No.402 dated 15.05.2019, the Committee is authorized to:

- Conduct, in the prescribed manner, inspections of compliance with the competition and natural monopoly legislation and, upon detection of breaches, institute proceedings and (or) consider such breaches;

Criterion 40.16

1894. In accordance with paragraphs 39, 40 of the Regulation approved by the CM Resolution of 29.06.2021 No. 402 provides that information obtained through international cooperation is used only for the purposes specified in the request or the response to such a request. Transfer of this information to state bodies or third parties or use of this information for administrative and criminal proceedings is only possible with the permission of the competent authority of the foreign state. However, there is no explicit requirement for the requesting authority to inform the requested authority without delay in cases where the requesting authority is obliged under national law to disclose or report the information received.

1895. According to Art.68(3) of Law No.ZRU-582 dated 11.11.2019, the Central Bank may disclose information received from a foreign country upon prior consent of a party that has provided such information and only for the purposes agreed by such party.

Criterion 40.17

1896. Uzbekistan is a party to a large number of bilateral cooperation agreements that provide for an exchange of information for combating crime, and is also a member of Interpol. According to the provided information, the Uzbek designated authorities actively exchange police information through the Interpol National Central Bureau.

1897. In Uzbekistan, information may be also exchanged internationally in the process of cooperation between the national and foreign tax authorities.

1898. A number of provisions have been added to the Uzbek legislation that give more legal certainty to the procedures related to exchange of information deemed a bank secret. In particular, Art.5 of Law No.520-II explicitly states that exchange of the relevant information between the prosecution, preliminary investigation and criminal intelligence authorities as well as sharing such information with foreign competent authorities in the prescribed manner does constitute unauthorized disclosure of bank secrets.

Criterion 40.18

1899. The Uzbek legislation allows for using the powers of competent authorities to provide international cooperation in terms of gathering information required for conducting inquiries and executing requests of foreign counterparts.

1900. The relevant provisions are set out in the criminal procedure legislation and in the legislation governing activities of competent authorities, inter alia, in Art.15 of Law No.ZRU-344 of Criminal Intelligence and Detective Activities dated 25.12.2012.

Criterion 40.19

1901. Until recently, there were no explicit legal provisions that enabled to form joint investigation teams, but, at the same time, no existing provisions precluded the establishment of such teams. Therefore, there was some legal uncertainly, which has been eliminated by the adoption of Resolution No.402 that empowers the LEAs to form joint investigation teams with participation of foreign law enforcement officers for conducting cooperative investigations into ML and associated predicate offences. Besides that, Uzbekistan is a party to a number of international treaties and agreements that

provide the opportunities of establishing such teams, sharing information and coordinating the joint actions.

1902. The Uzbek authorities drew attention to the fact that the MLA procedures in place allow officers of foreign competent authorities to attend to investigative proceedings (part 5 of article 595 of the CPC).

Criterion 40.20

1903. The Uzbek legislation does not explicitly prohibit the government authorities from pursuing international cooperation and establishing contacts with foreign competent authorities. Such contacts are established in practice, and the systems described above provide the sufficient regulatory mechanisms for their use.

Weighting and Conclusion

1904. In Uzbek legislation there is no explicit requirement for the requesting authority to inform the requested authority without delay in cases where the requesting authority is obliged under national law to disclose or report the information received.

1905. **Recommendation 40 is rated Largely Compliant.**

SUMMARY OF TECHNICAL COMPLIANCE – KEY DEFICIENCIES

Table Compliance with FATF Recommendations

Recommendations	Rating	Factor(s) underlying the rating
1. Assessing risks and applying a risk-based approach	LC	• The sector of the payment system operators does not have a requirement to provide information on the results of the risk assessment to the competent authority
2. National cooperation and coordination	C	All criteria are met
3. Money laundering offence	LC	• Insider deals and market manipulation, which are included in the established categories of offences in accordance with the FATF Recommendations, are not criminalized • Sanctions with respect to individuals is not proportional (coherent), and sanctions with respect to legal persons are limited to only one type of liability
4. Confiscation and provisional measures	LC	• The Republic of Uzbekistan does not criminalize insider deals and market manipulation, which excludes the application of confiscation of proceeds obtained as a result of these offences • Seizure of property as a provisional measure and confiscation of property is based solely on criminal procedural mechanisms
5. Terrorist financing offence	LC	• Uzbekistan's legislation does not criminalise the funding of de facto terrorist organisations which have not been recognised by a court decision as such or which are not included in UN sanctions lists • Providing funds to a person to pay for travel for training is not covered under the TF offence • Domestic law provides for a legal entity's only form of liability - its liquidation; such a sanction is not always proportionate and dissuasive
6. Targeted financial sanctions related to terrorism and terrorist financing	PC	• The Republic of Uzbekistan has not identified a competent authority responsible for submitting proposals on persons/entities to the relevant UNSC Committee • The principle of "without delay" application of the TFS is not fully ensured • The obligation to freeze funds (suspend transactions) and other assets are not envisaged for all physical and legal persons without exception • The immediate communication of information on designations to the financial sector and DNFBPs, as well as de-listing and unfreezing of assets, is not fully ensured • There are no requirements to protect bona fide third parties acting in a good manner
7. Targeted financial sanctions related to proliferation	PC	• In the legislation, the principle of "without delay" application of the TFS is not fully ensured

		• The obligation to freeze funds (suspend transactions) and other assets are not envisaged for all physical and legal persons without exception • There is no obligation to freeze without delay funds (suspend transactions) and other assets derived or generated through the use of funds or other assets that are owned (controlled) directly or indirectly by designated persons or entities • The immediate communication of information on designations to the financial sector and DNFBPs, as well as de-listing and unfreezing of assets, is not fully ensured • There are no requirements to protect bona fide third parties acting in a good manner • There is an unsettled issue of making payments under a contract entered into prior to the listing
8. Non-profit organizations (NPOs)	PC	• Comprehensive information from relevant sources was not used to determine the types of NPOs at risk of TF and the level of risk. The list of such sources was unnecessarily limited. • The NRA and SRA did not consider the threat posed to NPOs by terrorist entities • There was insufficient engagement with NPOs to develop and improve methods to identify and mitigate the risk of TF and related vulnerabilities • There is a lack of information on implementing special programs to encourage NPOs to conduct transactions through regulated financial channels • Administrative liability of NPOs as legal entities is not legislated
9. Financial institution secrecy laws	LC	• There are a number of legal restrictions for FIs to exchange information
10. Customer due diligence (CDD)	LC	• For banks and NBCIs the obligation to carry out CDD on threshold amounts is established not for all one-off transactions, but for their closed list • There are very limited statutory exemptions where no customer CDD is carried out when making a transfer • The legislation uses the term 'study' instead of 'understanding' of the client's ownership and management structure, which does not quite meet the requirement of the standards • There are deficiencies in the insurance sector related to confirming the identity of the recipient of the insurance benefit • The AML/CFT Law does not oblige financial institutions to carry out CDD of foreign structures without forming a legal entity considering their specificities • There is no legal provision for FIs (other than members of exchanges and operators, postal service

		providers) not to conduct CDD where there is suspicion of ML/TF, but instead to send an STR
11. Record keeping	LC	• For leasing and insurance companies, there are no provisions for storing the results of any analysis undertaken, with the exception of data obtained during CDD procedures
12. Politically exposed persons	PC	• The definition of PEP in the ICR for FIs does not include national PEPs, military positions and former PEPs of most FIs (except for banks and NBCIs) are not covered • Insurance and leasing companies are not assigned any responsibilities related to PEPs
13. Correspondent banking	LC	• Postal operators are not obliged to study the AML/CFT measures of companies providing international money transfer services however, the legislation requires not to enter into a relationship with an operator that does not comply with AML/CFT measures • In relation to the sector of payment organizations (payment organizations, electronic money system operators and payment system operators), norms of R.16 are not extended
14. Money or value transfer services (MVTS)	LC	• There is no requirement in the legislation to license postal money order services, to apply sanctions for unlicensed activities in this sector, to maintain a register of payment agents and transfer it to the regulator
15. New technologies	LC	• There are no requirements to prevent criminals and their accomplices from entering the VASP beneficial ownership • There is no direct requirement for applying sanctions not only to VASPs, but also to their directors and senior managers • There are no rules on the exchange of supervisory information related to AML
16. Wire transfers	LC	• There are very limited exemptions in the legislation on the amounts and cases when money transfers and electronic money transfers are not accompanied by the required sender and recipient information • In Uzbekistan information about the originator and beneficiary does not always accompany the transfer, while other means are not used • There is no procedure for follow-up in case of detection of money transfers without the required beneficiary and (or) originator information • For postal operators no requirements to perform R.16 in countries where they carry out their activities directly or through agents
17. Reliance on third parties	LC	• There is no indication in the ICR of payment organizations, electronic money system operators, payment system operators that when relying on third

		parties, the ultimate responsibility for customer due diligence is borne by the organizations themselves
18. Internal controls, foreign branches and subsidiaries	PC	• In financial institutions, the AML/CFT official does not belong to the management team and for the main FI is limited to the position of the head of the internal control service • There are no requirements for the qualifications and business reputation of the FI employees (except for AML/CFT units, heads of banks and NBCIs) • There are no requirements for business reputation of AML/CFT responsible persons for exchange members and leasing organizations • Internal audit of AML/CFT systems is established only for banks and NBCIs • FIs (except for banks) do not use group AML/CFT programmes
19. Higher risk countries	LC	• Possible countermeasures for FIs (with the exception of banks and NBCIs) have not been developed against States that do not participate in international cooperation in the field of AML/CFT, with the exception of filing STRs and applying CDD measures. • There is no statutory requirement to apply enhanced CDD measures commensurate with the risks.
20. Reporting of suspicious transactions	C	All criteria are met
21. Tipping-off and confidentiality	LC	• The lack of a direct indication in the legislation that the provision of information cannot be the basis for liability regardless of whether the illegal activity actually took place, carries risks associated with the emergence of liability of the organization or its employees to third parties
22. DNFBPS: customer due diligence	PC	• Deficiencies in relations with national PEPs, a number of DNFBPs lack the obligation to file an STR when they cannot conduct CDD • Organizations performing the duties of an agent to establish legal entities are not subject to AML/CFT/CPF requirements
23. DNFBPS: other measures	LC	• There are deficiencies related to implementing the R.18 requirements • Some deficiencies under R.21 (notary offices and lawyers' groups)
24. Transparency and beneficial ownership of legal persons	LC	• Legal persons are not required to obtain and maintain information on their BO. • Liability and sanctions cover only a small portion of possible violations and are not considered by assessors to be proportionate and dissuasive
25. Transparency and beneficial ownership of legal arrangements	PC	• Measures envisaged by the current legislation in relation to foreign trusts, in particular those connected with keeping information about the

		beneficiary, as well as the requirements for CDD measures (except for banks), seem insufficient
26. Regulation and supervision of financial institutions	PC	• For FIs (except banks and NBCIs) there are no requirements to business reputation of beneficial owners, founders and senior managers • Business reputation requirements do not apply to persons associated (affiliated) with the beneficial owners and senior managers of all FIs • Founders and shareholders of a bank, a microcredit organization are considered non-compliant in limited cases (not for all types of offences) • There is no information on consolidated supervision organization in the securities sector • There are no risk-based AML/CFT supervision (except CB) and connection of annual ML/TF/PF risk assessment with the activities of FIs (except for banks, payment institutions, NBCIs) • Insurance agents, postal operators and providers, mobile money transfer operators, leasing organisations are not subject to licensing and/or registration
27. Powers of supervisors	LC	• The supervisors for exchange members have no authority to conduct inspections • The supervisor of insurance companies does not have the power to request any information other than that requested during inspections • The set of sanctions from the Insurance Market Development Agency under the Finance Ministry is limited • The AML/CFT component is not highlighted in the list of sanctions of the DCMD, Ministry of Finance.
28. Regulation and supervision of DNFBPS	LC	• There are no requirements for beneficial owners and persons owning controlling interests, and the licensing requirements do not apply to persons affiliated with criminals
29. Financial intelligence units	C	All criteria are met
30. Responsibilities of law enforcement and investigative authorities	C	All criteria are met
31. Powers of law enforcement and investigative authorities	C	All criteria are met
32. Cash couriers	C	All criteria are met
33. Statistics	LC	The statistics are maintained not in full scope and cannot be considered comprehensive
34. Guidance and Feedback	LC	There is no mechanism in place for providing specific recommendations regarding STR quality feedback
35. Sanctions	PC	Sanctions for violations of the AML/CFT requirements for legal persons are limited

36. International Instruments	LC	• The confiscation regime requires improvement, as it is limited to restitution and seizure of material evidence only. • Besides that, the deficiencies in R.12 related to requirements for financial institutions to identify politically exposed persons (PEPs) impact the full implementation of Merida Convention.
37. Mutual Legal Assistance	C	All criteria are met
38. Mutual Legal Assistance: Freezing and Confiscation	LC	• The possibility of actually enforcing a foreign request for non-conviction-based confiscation is limited • Enforcement of confiscation judgments may be based on a limited number of international treaties, as well as on the principle of reciprocity
39. Extradition	C	All criteria are met
40. Other Forms of International Cooperation	LC	• There is no explicit requirement for the requesting authority to inform the requested authority without delay in cases where the requesting authority is obliged under national law to disclose or report the information received

GLOSSARY OF ACRONYMS

	DEFINITION
AML/CFT Law	Law of the Republic of Uzbekistan No. 660-II of 26.08.2004 "On Counteraction of Legalization of Proceeds of Crime, Financing of Terrorism and Financing Weapons of Mass Destruction Proliferation" (as amended by Law of the Republic of Uzbekistan No. LRU-516 of January 15, 2019)
AML/CFT/PF	Anti-Money Laundering/Countering the Financing of Terrorism and Financing of Proliferation of weapons of mass destruction
Bank	Commercial bank
BCE	Bureau of Compulsory Enforcement under the General Prosecutor's Office
BO	Beneficial owner
BPC	Bank payment card
CAO	Administrative Liability Code of the Republic of Uzbekistan
CB, Central Bank	Central Bank of the Republic of Uzbekistan
CC, Criminal Code	Criminal Code of the Republic of Uzbekistan
Civil Code	Civil Code of the Republic of Uzbekistan
CHFIU	Council of Heads of Financial Intelligence Units of the Commonwealth of Independent States
CM	Cabinet of Ministers of the Republic of Uzbekistan
CPC	Criminal Procedure Code of the Republic of Uzbekistan
Customs Code	Customs Code of the Republic of Uzbekistan
DCEC	Department for Combating Economic Crimes under the Office of the Prosecutor General of the Republic of Uzbekistan, Uzbekistan’s FIU
DCMD	Department for Capital Market Development under the Ministry of Finance of the Republic of Uzbekistan
DPMS	Dealers in precious metals and stones
EDD	Enhanced due diligence
E-HAT	E-HAT secure email system
FI	Financial institution
FTF	Foreign terrorist fighter
GPO	Office of the General Prosecutor of the Republic of Uzbekistan
IAC	Interdepartmental Commission on Combating the Legalization of the Proceeds of Crime, the Financing of Terrorism and the Financing of Proliferation of Weapons of Mass Destruction
ICR	Rules of internal control
ITO	International terrorist organization

LEA	Law enforcement authority
MCO	Microcredit organization
MD	Ministry of Defense of the Republic of Uzbekistan
MIA	Ministry of Internal Affairs of the Republic of Uzbekistan
MITCD	Ministry of Information Technology and Communications Development of the Republic of Uzbekistan
MJ, Justice Ministry	Ministry of Justice of the Republic of Uzbekistan
MF, Finance Ministry	Ministry of Finance of the Republic of Uzbekistan
MFA	Ministry of Foreign Affairs of the Republic of Uzbekistan
MLA	Mutual legal assistance
NAPM	National Agency for Project Management under the President of the Republic of Uzbekistan
NBCI	Non-banking credit institution
NLA	Normative-legal act, normative-legal acts
NPO	Non-profit organization (in Uzbekistan: Non-government Non-profit organization)
NRA	National risk assessment of money laundering and terrorism financing
Oliy Majlis	Oliy Majlis (Parliament of the Republic of Uzbekistan)
OIA	Operational investigative activity, criminal intelligence and detective activity (activities carried out publicly and covertly by authorised LEA's units to detect, suppress or solve crimes, locate fugitives and missing persons, identify property liable to confiscation, obtain information on events and acts dangerous to the State)
OIM	Operational investigative means, criminal intelligence and detective operations (actions carried out by authorised LEA's units, which are based on the use of public and covert means, aimed at solving specific tasks of the OIA)
PCD	Passenger customs declaration
RSV	Reference settlement value - an indicator determined in Uzbekistan by Presidential Decree for the purposes of criminal and administrative liability (determining the amounts of fines, damages, criminal incomes, etc). RSV on 02.07.2021 was 245,000 soums (about 23 USD).
RUACE	Republican Universal Agricultural Commodity Exchange
SAC	State Assay Chamber under the Ministry of Finance of the Republic of Uzbekistan
SC	Supreme Court of the Republic of Uzbekistan
SCC	State Customs Committee of the Republic of Uzbekistan
SRA	Sectoral risk assessment
SSRBE	Single State Register of Business Entities
SSS	State Security Service of the Republic of Uzbekistan

STC	State Tax Committee of the Republic of Uzbekistan
TFS	Targeted financial sanctions
UNCE	Uzbek National Commodity Exchange
UNSC	UN Security Council
UNSCR	UN Security Council Resolution
UzSAMA	Uzbekistan State Assets Management Agency
UZEX	Uzbek commodity exchange
VA	Virtual assets
VASP	Virtual Asset Service Provider